УДК 004.056.5

В. Б. Дудикевич, Г. В. Микитин, Т. Б. Крет
Національний університет “Львівська політехніка”,
кафедра захисту інформації

УНІВЕРСАЛЬНА ПЛАТФОРМА СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У БАГАТОРІВНЕВИХ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КЕРУВАННЯ

© Дудикевич В. Б., Микитин Г. В., Крет Т. Б., 2016

Запропоновано теоретико-методологічну модель універсальної платформи побудови системи захисту інформації у багаторівневих інтелектуальних системах керування (БІСК). Розроблено моделі інформаційно-технічних станів БІСК. Створено модель загроз та модель системи захисту інформації в БІСК.

Ключові слова: багаторівнева інтелектуальна система керування, система захисту інформації, універсальна платформа, загрози, моделі.

Theoretical and methodological model of a universal platform building information security system in multi-level intelligent control system is proposed. The model of the information-technical position multi-level intelligent control system has been developed. Model of threats and model of information security system has been developed.

Key words: multi-level intelligent control system, information security system, vulnerability, models.

Вступ

Закони України “Про інноваційну діяльність” та “Про пріоритетні напрями інноваційної діяльності в Україні” заклали стратегію формування, діяльності і розвитку нових та конкурентоспроможних технологій. Актуальними сьогодні є завдання аналізу та обробки даних, прийняття рішення на керування об’єктами та ситуаціями. Ці задачі ефективно розв’язуватимуться із застосуванням інтелектуальних засобів, зокрема інтелектуальних систем керування, що застосовуються у різних предметних галузях сучасної інфраструктури суспільства.

Актуальним стає впровадження інтелектуальних об’єктів у площинах промисловості та енергетики, зокрема у контексті реалізації концепції Smart Grid, що потребує створення багаторівневих інтелектуальних систем керування (БІСК) та створення систем захисту інформації (СЗІ) у межах Стратегії кібербезпеки України [1, 2].

Постановка задачі

З метою виконання завдань інтелектуалізації суспільства засобами інтелектуальних технологій у контексті контролю стану об’єктів, аналізу і обробки даних, передавання і приймання інформації безпровідними мережами і прийняття рішення на управління інтелектуальними об’єктами доцільно використовувати багаторівневі інтелектуальні системи керування.

Мета роботи – створити універсальну платформу побудови системи захисту інформації в БІСК у просторі “відбір/контроль – аналіз/обробка – передавання/приймання – управління”; побудувати просторові моделі інформаційно технічних станів БІСК; створити інтегральну модель загроз інформаційній безпеці та модель системи захисту в БІСК.

Універсальна платформа СЗІ в БІСК: засади створення

Умова безпечного функціонування БІСК. Контроль стану безпеки системи об'єктів здійснюється БІСК згідно з умовою безпечного функціонування самих інтелектуальних систем на рівні: контролю, обробки, передавання/приймання інформації та керування (СОУ Н НКАУ 0060: 2010):

$$j_K(P_1^t,...P_n^t,Z_1^t,...Z_m^t) \le d^t, \quad (1)$$

де j_K – функція контролю системи; P_i^t – параметри системи, що контролюються; Z_j^t – умовні контрольні значення параметрів дестабілізуючих факторів: дефекти розроблення або проектування (ДР); фізичні дефекти (ДФ); дефекти зовнішніх впливів або взаємодій (ДВ); d^t – граничне значення j_K, що визначає умову роботоздатного стану системи.

Модель функціональної безпеки БІСК на рівні безвідмовності. Модель безвідмовності системи керування пов'язана з властивостями готовності, обслуговуваності, збереженості, надійності та іншими властивостями гарантоздатності БІСК, наприклад, збереженості та довговічності (СОУ Н НКАУ 0060: 2010). Умова забезпечення безвідмовності (гарантоздатності) – це комплекс параметрів БІСК, які забезпечують функціональну роботоздатність за винятком можливості виходу системи за граничний стан на рівні: контролю, обробки, передавання/приймання інформації, керування:

$$f(P_i,C_P,n_s,n_m,T_{ef}) \ge 0, \quad (2)$$

де $f(\bullet)$ – функція параметрів БІСК; за умови $f(\bullet)<0$ інтелектуальна система керування переходить в позаграничний стан; P_i – розрахункові значення параметрів системи за технічним завдання (під час розроблення/проектування); C_P – обмеження на контрольований параметр, наприклад (допустиме значення контролю стану об'єкта); n_s – коефіцієнт надійності інтелектуальної системи, що враховує можливі наслідки відмови; n_m – коефіцієнт надійності моделі БІСК, який враховує невизначеність розрахункової, наприклад, недосконалість розроблення / проектування; T_{ef} – встановлений термін ефективної експлуатації системи за технічним завданням.

Універсальна платформа створення СЗІ в БІСК. Основними методологічними принципами архітектурної реалізації ІСК є ситуаційне керування та обробка даних. Серед технологій створення ІСК використовують експертні системи, штучні нейронні мережі; нечітку логіку; еволюційні методи та генетичні алгоритми.

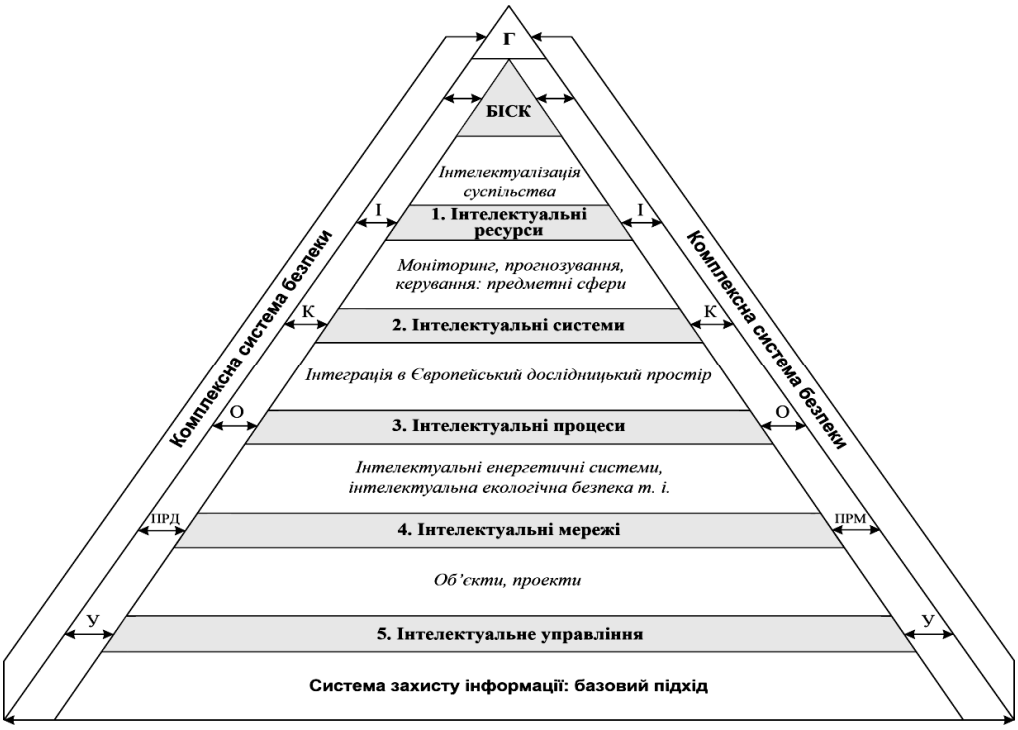

Рис. 1. Структура універсальної платформи СЗІ в БІСК

Сьогодні успішно функціонують БІСК у різних предметних сферах, зокрема, це: багаторівнева інтелектуальна інформаційна система опрацювання відеоконтенту для осіб з вадами зору у галузі охорони здоров'я, інтелектуальна система керування з багаторівневим перетворенням інформації на авіаційному підприємстві у сфері перевезень та логістики, інтелектуальні системи управління мобільними радіомережами військового призначення, де використана ієрархічна модель побудови. Для кожної з наведених структур ІСК, створених за відповідними технологіями, характерна своя багаторівневість у контексті виконання функціональних завдань у предметних сферах. Ступінь захищеності багаторівневих інтелектуальних систем керування зумовлений їх архітектурою, функціональними особливостями, впливом загроз, механізмами безпеки (ISO/IEC 15408). Концепція побудови СЗІ зумовлена універсальною платформою подання інтелектуальної системи керування цілісною багаторівневістю, що охоплює елементи структурованості та функціональності.

З позиції структурованості БІСК розглянуто як: 1) інтелектуальні ресурси, що формують сегмент інтелектуалізації суспільства; 2) інтелектуальні системи як інтструментарій реалізації відбору інформації, моніторингу, прогнозування і керування; 3) інтелектуальні процеси на рівні інтеграції в європейський дослідницький простір; 4) інтелектуальні мережі, зокрема у контексті підвищення ефективності енергоспоживання та використання відновлювальних джерел енергії; інтелектуальне управління, зокрема розподіленими у просторі динамічними об'єктами, автономними мобільними кібернетичними системами, соціально-економічними процесами тощо.

З позиції функціональності БІСК розглянуто як: 1) контроль стану об'єктів на рівні відбору параметрів та обробки інформації (К, О); 2) передавання / приймання даних (ПРД / ПРМ); 3) управління станом об'єктів (У). Методологічним підґрунтям побудови системи захисту інформації в БІСК є створення базового підходу, одним з сегментів якого є побудова комплексних систем безпеки на рівні "багаторівнева інтелектуальна система керування – багаторівневий захист" на основі концепції "об'єкт – загроза – захист". Відповідно до архітектури БІСК розглянемо базовий підхід до побудови СЗІ в БІСК, цільовим спрямуванням якого є виконання завдань безпеки інтелектуальних технологій – забезпечення конфіденційності, цілісності, доступності, спостережуваності, гарантій у просторі інтелектуалізації міжнародної спільноти.

Підґрунтям створення універсальної платформи СЗІ в БІСК є: універсальна структура БІСК – інтелектуальні ресурси (ІР), інтелектуальні системи (ІС), інтелектуальні процеси (ІП), інтелектуальні мережі (ІМ), інтелектуальне управління (ІУ); базовий підхід до захисту інформації в БІСК; комплексні системи безпеки у просторі "інформація – контроль/обробка – передавання/приймання – управління" (рис. 1).

Розглянемо основні компоненти базового підходу до побудови СЗІ в БІСК:

– функціональна архітектура БІСК з відображенням властивостей предметних сфер;

– комплекс моделей: модель інформаційно-технічних станів БІСК за умови факторів впливу на систему, модель загроз, модель багаторівневого захисту БІСК;

– структура СЗІ за матричним методом у просторі "основи – напрями – етапи" для універсальної структури БІСК "ІР – ІС – ІП – ІМ – ІУ";

– оцінювання ефективності СЗІ у межах стандартизованої методики відповідно до обгрунтованого методу побудови СЗІ в БІСК.

Моделі інформаційно технічних станів БІСК: концепція "об'єкт – загроза – захист"

Модель інформаційно-технічних станів (ІТС) БІСК у просторі "К, О – ПРД/ПРМ – У". На рис. 1 показано просторові моделі інформаційно-технічних станів БІСК відповідно до концепції "об'єкт – загроза – захист". Ці моделі пов'язані із забезпеченням гарантоздатності БІСК у площинах їх функціональної та інформаційної безпеки. Гарантоздатність – це комплексна властивість системи надавати необхідні послуги, яким можна довіряти. Структура гарантоздатності (СОУ-Н НКАУ 0060:2010) включає такі складові: первинні властивості; загрози функціональній роботоздатності; відмовостійкість; вторинні властивості; взаємозв'язки між складовими. До первинних властивостей гарантоздатності належать: безвідмовність, готовність, обслуговуваність, живучість, функціональна

безпека, цілісність, конфіденційність, вірогідність. Гарантоздатність та інформаційна безпека взаємопов'язані на рівні загальних властивостей – цілісності і конфіденційності та специфічних – автентичності і достовірності. Відповідно до концепції "об'єкт – загроза – захист", об'єктом захисту є інформація, яка циркулює в БІСК, що представлена як універсальна структура – ІС, ІП, ІУ (вверху) ІМ (посередині), ІР (внизу). Комплекс загроз (1 – 2 – 3) відповідає впливу дестабілізуючих факторів ДР, ДФ та ДВ на універсальну структуру БІСК. Інформаційно-технічний стан системи – це сукупність властивостей та ознак як технічного, так і інформаційного характеру про придатність системи у певний момент часу (СОУ-Н НКАУ 0060:2010). Стани системи, що зумовлені впливом загроз ДР, ДФ та ДВ, класифікують як: працездатний (безпечний), частково працездатний (безпечний), непрацездатний (безпечний), непрацездатний (небезпечний). Саме у такому контексті розглянемо модель простору ІТС за умови впливу комплексу загроз функціональній та інформаційній безпеці БІСК (рис. 2, *а – г*).

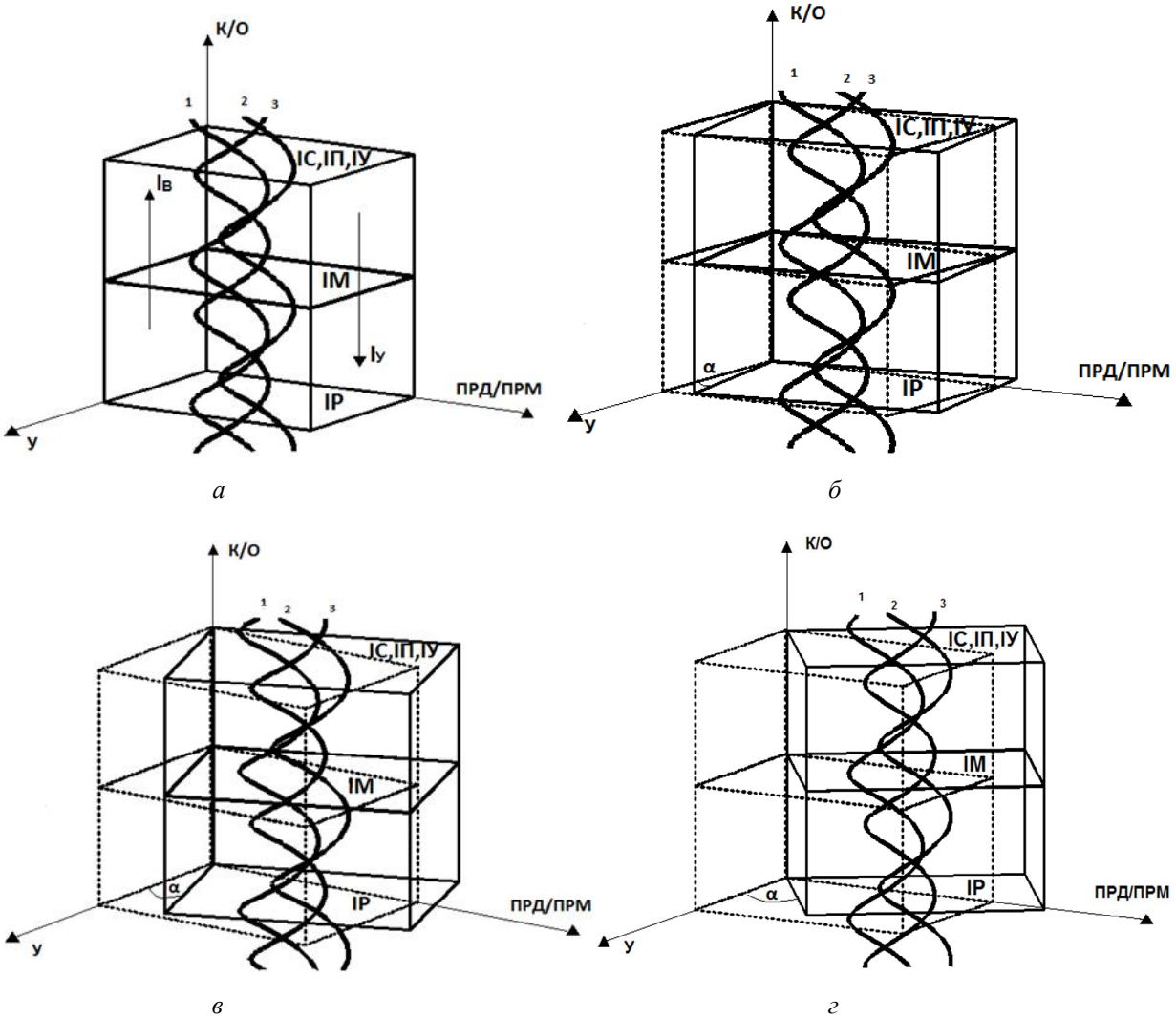

Рис. 2. Модель простору інформаційно-технічних станів БІСК у контексті гарантоздатності: а – працездатний (безпечний) стан – NORMA; б – частково працездатний (безпечний) стан – ALARM-1; в – непрацездатний (безпечний) стан – ALARM-2; г – непрацездатний небезпечний стан – AVARIA

Інформаційно-технічні стани взаємопов'язані у контексті гарантоздатності взаємозалежністю функціональної та інформаційної безпеки: внаслідок порушення конфіденційності, як одного з профілів інформаційної безпеки, реалізується несанкціонований доступ до інформації у системі керування, що позиціонується як перехід системи у непрацездатний небезпечний стан, який на функціональному рівні означає: пошкодження, збій, відмову апаратних або програмних засобів. Згідно з універсальною структурою БІСК "ІР – ІС – ІП – ІМ – ІУ" (рис. 1) модель інформаційно-

технічних станів подано у функціональному просторі “К, О – ПРД/ПРМ – У” (рис. 2). Вплив загроз ДР (1), ДФ (2), ДВ (3) на функціональну багаторівневість ІСК, які з великою ймовірністю виявляються та блокуються комплексною системою безпеки, характеризується множиною працездатних безпечних станів МСПС (рис. 2, а). Якщо загрози ДР (1), ДФ (2), ДВ (3), що впливають на БІСК, не виявляються та не блокуються (нейтралізуються) системою безпеки, то це призводить до зміни інформаційно-технічного стану системи, що умовно можна зобразити її переміщенням у просторі “К, О – ПРД/ПРМ – У” проти годинникової стрілки (рис. 2, б, в, г) та охарактеризувати множиною частково працездатного (безпечного) стану МСПС (рис. 2, б), множиною непрацездатного (безпечного) МСНП-БС (рис. 2, в), множиною непрацездатного (небезпечного) МСНП-НБС (рис. 2, г).

Ефективність функціональної та інформаційної безпеки у контексті забезпечення конфіденційності, цілісності та доступності інформації в БІСК зумовлюється багаторівневістю системи захисту інформації, що забезпечить відмовобезпечність системи керування для інтелектуальної інфраструктури суспільства. Побудова СЗІ в БІСК ґрунтується на моделі загроз, моделі порушника, моделі багаторівневої безпеки.

Інтегральна модель загроз, модель захищеної БІСК. Комплексна система безпеки інтелектуальних систем керування, яка спрямована на забезпечення міцності захисту інформації, ґрунтується на моделі загроз; моделі порушника; проектуванні системи безпеки. Технологія проектування системи захисту в інформаційних системах здійснюється згідно з завданням забезпечення безпеки – конфіденційності, цілісності, доступності, спостережуваності, гарантій та їх взаємозв’язку відповідно до ISO/IEC 15408. Одним з універсальних методів як побудови системи захисту інформації, так і оцінювання її ефективності, є матричний метод. Цей метод описує модель інформаційної безпеки БІСК за трьома сегментами: основи (О), що розкривають структуру СЗІ за нормативно-правовою, організаційною, інформаційною та іншими складовими; напрямки захисту (Н), які відображають функціональне призначення; етапи створення (Е), які формують ступінь забезпечення завдань безпеки. Етапи створення СЗІ передбачають: визначення інформаційних і технічних ресурсів, які підлягають захисту; виявлення множини імовірних загроз і каналів витоку інформації; проведення оцінки уразливості та ризиків інформації за дії комплексу загроз та активності каналів витоку; обґрунтування вимог до системи захисту; оптимізація критеріїв вибору засобів захисту у контексті їх характеристик; впровадження вибраних заходів, способів та засобів; реалізація контролю цілісності та управління системою захисту. Кількість елементів матриці (К) визначається

$$K = O_i \cdot H_j \cdot E_k, \tag{3}$$

де O_i, H_j, E_k – відповідно кількість складових сегментів матриці – основи, напрямки, етапи.

Інтегральна модель загроз функціональній та інформаційній безпеці БІСК (СОУ Н НКАУ 0060: 2010):

$$Q = \{MZ_i^L, i \in I; MZ_j^N, j \in J; MZ_k^S, k \in K\}, \tag{4}$$

де I – структура СЗІ для виявлення множини загроз на рівні ДР; J – структура СЗІ для виявлення множини загроз на рівні ДФ; S – структура СЗІ для виявлення множини загроз на рівні ДВ; MZ_i^L, MZ_j^N, MZ_k^S – відповідно множини загроз, що виявляються структурами СЗІ в БІСК.

Модель системи захисту інформації в БІСК згідно з багаторівневою безпекою:

$$G = \{MZ_k^{SVUD}, k \in K\}, \tag{5}$$

де MZ_k^{SVUD} – множина технологій виявлення, блокування (нейтралізації) загроз інформаційній безпеці (S) відповідно до профілів захисту: конфіденційності (V), цілісності (U), доступності (D), які характерні для кожного з рівнів інформаційної безпеки. Одним із способів реалізації багаторівневого захисту інформації в БІСК є автоматизована система керування взаємопов’язаними перепонами, яка спрямована на забезпечення міцності захисту інформації в БІСК за допомогою перекривання імовірних каналів НСД та впливів відповідно до моделі потенційного порушника, що

унеможливлює несанкціоноване ознайомлення з даними, їх модифікацію та знищення за рахунок періодичного контролю блоком управління давачів, що забезпечують виявлення і блокування (нейтралізацію) НСД. Багаторівневий захист задовольняє вимоги забезпечення ефективності інформаційної та функціональної безпеки: 1) кожний з рівнів є багатоланковим – системи контролю доступу у приміщення, системи захисту від побічного електромагнітного випромінювання і наведення, системи криптографічного захисту; 2) міцність захисної перепони (багаторівневого захисту) є достатньою, якщо очікуваний час подолання її порушником більший від часу життєвого циклу інформації в БІСК та більший від часу виявлення і блокування його несанкціонованого доступу.

Висновки

Розроблено універсальну платформу створення систем захисту інформації в інтелектуальних технологіях на рівні універсальної структури БІСК “інтелектуальні ресурси – інтелектуальні системи – інтелектуальні процеси – інтелектуальні мережі (канали) – інтелектуальне управління”, відповідно до функцій: контролю/обробки, передавання/приймання, управління. Створено моделі просторових інформаційно-технічних станів БІСК за умов впливу комплексу дестабілізуючих факторів. Розроблено інтегральну модель загроз для БІСК та створено модель системи захисту інформації в БІСК для забезпечення багаторівневої безпеки.

1. Sample of European Smart Grids Projects [Електронний ресурс]. – Режим доступу: http://www.smartgrids.eu/EU_Projects. 2. Указ Президента України від 15 березня 2016 року № 96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”.