УДК 004.056

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

Національний університет "Львівська політехніка", Львів

КОНЦЕПЦІЯ ТА БАЗОВИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БАГАТОРІВНЕВІЙ ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ КЕРУВАННЯ

Розроблено концепцію створення системи захисту інформації (СЗІ) в багаторівневій інтелектуальній системі керування (БІСК) на основі структури "багаторівнева система – багаторівневий захист". Запропоновано базовий підхід до побудови СЗІ в БІСК на основі принципів системного аналізу: архітектура БІСК – модель загроз, модель інформаційно-технічних станів системи, модель захищеної БІСК – структура СЗІ – оцінювання ефективності СЗІ.

Ключові слова: *багаторівнева інтелектуальна система, система захисту інформації, модель, метод, оцінювання ефективності.*

Вступ

Актуальність. В процесі розвитку інноваційних проектів в рамках "Україна – ЄС" – "Інтелектуальні енергетичні системи", "Інтелектуальна екологічна безпека" та інших актуальним залишається сегмент функціональної та інформаційної безпеки інтелектуальних технологій, як основного інструментарію забезпечення безпечного функціонуванню суспільства в 21–му столітті, зокрема у контексті: управління ризиками надзвичайних ситуацій *на рівні: концепції* Державної служби України з надзвичайних ситуацій та Міжнародної організації управління ризиками; моніторингу та прогнозування зміни земного клімату та прийняття рішення на управління *за декларацією* клімат-саміту-2015; радіаційного моніторингу та управління ядерною безпекою *за напрямами діяльності МАГАТЕ*; розроблення та впровадження інтелектуальних енергетичних мереж *за концепцією Smart Grid* та *згідно Європейської платформи розумних електромереж*.

Постановка задачі і мета роботи. Основні наукові задачі: розроблення концепції та базового підходу до створення СЗІ в багаторівневих інтелектуальних систем керування згідно: пріоритетних напрямів та досліджень Проекту концепції інформаційної безпеки України; трикомпонентної структури програми ЄС з досліджень та інновацій "передова наука – індустріальне лідерство – соціальні виклики"; нормативної бази у галузі забезпечення безпеки автоматизованих систем.

Мета роботи – розроблення методологічних засад створення СЗІ в багаторневих інтелектуальних системах керування.

Основний матеріал

Гарантоздатність БІСК. Гарантоздатність – це комплексна властивість системи надавати необхідні послуги, яким можна оправдано 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 відносяться: безвідмовність, готовність, обслуговуваність, живучість, функціональна безпека, цілісність, конфіденційність, вірогідність. Гарантоздатність та інформаційна безпека взаємозв'язані на рівні загальних властивостей – цілісності і конфіденційності та специфічних – автентичності і достовірності. Функціональна безпека спрямована на створення моделей захисту інформаційних систем на основі методів і засобів апаратно-програмного забезпечення відповідно до ймовірних загроз: невизначеність; відмова; аварія. Інформаційна безпека – спрямована на створення моделей захисту інформаційних систем на основі методів і засобів апаратно-прогамного забезпечення відповідно до ймовірних загроз: витік; модифікація; знищення.

Неповнота / відсутність забезпечення гарантоздатності автоматизованих систем та програмного забезпечення на рівні кожної з її властивостей призводить до: дефектів, помилок, відмов, що відповідно знижує рівень вирішення проблеми забезпечення безпеки об'єктів у різних предметних сферах. Рівень гарантоздатності автоматизованих систем визначають: дефекти розроблення / проектування (ДР), які характерні для програмного забезпечення; фізичні дефекти (ДФ), що характерні для апаратного забезпечення; дефекти зовнішніх впливів / взаємодій (ДВ), які є наслідком несанкціонованого доступу (інформаційних атак), помилок персоналу, впливу фізичних факторів, які можуть призвести до кратних відмов апаратних і програмних засобів.

Умова безпечного функціонування БІСК. Контроль стану безпеки об'єктів здійснюється БІСК згідно умови безпечного функціонування самих інтелектуальних систем на рівні: контролю, обробки, пе-

редавання/приймання інформації та керування (СОУ Н НКАУ 0060: 2010)

$$\varphi_K(P_1^t,...P_n^t,Z_1^t,...Z_m^t) \le \delta^t,$$

де φ_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); δ^t – граничне значення φ_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 з виключенням можливості виходу системи за граничний стан на рівні: контролю, обробки, передавання/приймання інформації, керування

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

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.

Концепція створення СЗІ в БІСК. Підґрунтям створення концепції побудови СЗІ в БІСК є структура "універсальна платформа БІСК – базовий підхід до захисту" (рис. 1).

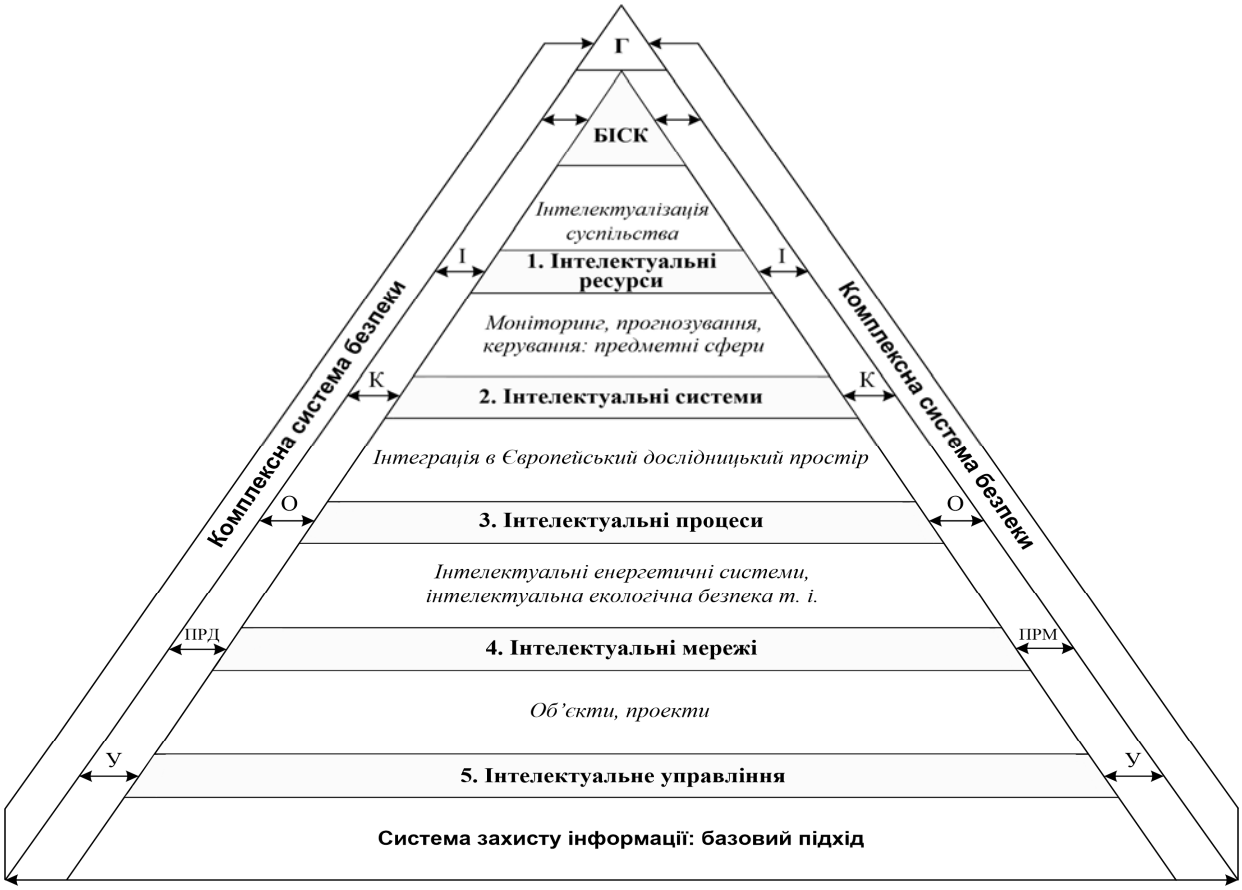

Рис. 1. Структура концепції побудови СЗІ в БІСК

Універсальна платформа 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. На сьогодні успішно функціонують БІСК в різних предметних сферах, зокрема це: багаторівнева інтелектуальна інформаційна система опрацювання відеоконтенту для осіб з вадами зору у галузі охорони здоров'я [1],

інтелектуальна система керування з багаторівневим перетворенням інформації на авіаційному підприємстві у сфері перевезень та логістики [2], інтелектуальні системи управління мобільними радіомережами військового призначення, де використана ієрархічна модель побудови [3]. Для кожної з наведених структур ІСК, створених за відповідними технологіями, характерна своя багаторівневість у контексті виконання функціональних задач у предметних сферах.

Ступінь захищеності багаторівневих інтелектуальних систем керування обумовлений їх архітектурою, функціональними особливостями, впливом загроз, механізмами безпеки (ISO/IEC 15408). Концепція побудови СЗІ обумовлена універсальною платформою представлення інтелектуальної системи керування цілісною багаторівневістю, що охоплює елементи структурованості та функціональності.

З позиції структурованості БІСК розглянуто, як: 1) інтелектуальні ресурси (ІР), що формують сегмент інтелектуалізації суспільства; 2) інтелектуальні системи (ІС), як інструментарій реалізації відбору інформації, моніторингу, прогнозування і керування; 3) інтелектуальні процеси (ІП) на рівні інтеграції в Європейський дослідницький простір; 4) інтелектуальні мережі (ІМ), зокрема у контексті реалізації концепції *Smart Grid*, спрямованої на підвищення ефективності енергоспоживання та використання відновлювальних джерел енергії; інтелектуальне управління (ІУ), зокрема розподіленими у просторі динамічними об'єктами, автономними мобільними кібернетичними системами, соціально-економічними процесами т.ін.

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 вирішення задач безпеки інтелектуальних технологій – забезпечення конфіденційності, цілісності, доступності, спостережуваності, гарантій у просторі інтелектуалізації міжнародної спільноти.

Базовий підхід до побудови СЗІ в БІСК. Базовий підхід у частині взаємозв'язку гарантоздатності з інформаційною безпекою на рівні задач забезпечення конфіденційності, цілісності, доступності має ієрархічну структуру: архітектура та функціональні можливості БІСК у предметній сфері – взаємозв'язок моделі простору інформаційно-технічних станів, моделі загроз та моделі захищеної БІСК – обґрунтування вибору методу побудови СЗІ – оцінювання ефективності СЗІ та прийняття рішення щодо її покращення (рис. 2).

Рис. 2. Структура базового підходу до побудови СЗІ в БІСК

Модель простору інформаційно-технічних станів (ІТС) 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 обумовлюються впливом загроз ДР, ДФ та ДВ класифікують, як: працездатний (безпечний), частково працездатний (безпечний), непрацездатний (безпечний), непрацезданий (небезпечний).

Саме у такому контексті розглянемо модель простору ІТС за умови впливу комплексу загроз функціональній та інформаційні безпеці БІСК (рис. 3, а – г). Інформаційно-технічний стани взаємо-

пов'язані в контексті гарантоздатності взаємозалежністю функціональної та інформаційної безпеки: внаслідок порушення конфіденційності, як одного з профілів інформаційної безпеки, реалізується несанкціонований доступ до інформації в системі керування, що позиціонується, як перехід системи в непрацездатний небезпечний стан, який на функціональному рівні означає – пошкодження, збій, відмова апаратних або програмних засобів.

Згідно універсальної платформи БІСК "ІР – ІС – ІП – ІМ – ІУ" (рис. 1) модель інформаційно-технічних станів представлена у функціональному просторі "К, О – ПРД/ПРМ – У" (рис. 3).

Вплив загроз ДР (1), ДФ (2), ДВ (3) на функціональну багаторівневість ІСК, які з великою імовірністю виявляються та блокуються комплексною системи безпеки характеризується множиною працездатних безпечних станів $MS_{ПС}$ (рис. 3, 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. 3, б, в, г) та охарактеризувати: множиною частково працездатного (безпечного) стану $MS_{ПС}$ (рис. 3, б), множиною непрацездатного (безпечного) $MS_{НП\text{-}БС}$ (рис. 3, в), множиною непрацездатного (небезпечного) $MS_{НП\text{-}НБС}$ (рис. 3, г). З метою забезпечення функціональної та інформаційної безпеки у контексті задач конфіденційності, цілісності та доступності, необхідно обґрунтувати критерії вибору системи захисту інформації в БІСК, представити її багаторівневою структурою, що обумовить відмовобезпечність системи керування.

Інтегральна модель загроз, модель порушника, 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 задач забезпечення безпеки – конфіденційності, цілісності, доступності, спостережуваності, гарантій та їх взаємозв'язку у відповідності до ISO/IEC 15408 [4]. Одним з універсальних методів як побудови системи захисту інформації, так оцінювання її ефективності є матричний метод [5]. Цей метод описує модель інформаційної безпеки БІСК за трьома сегментами: основи (*O*), що розкривають структуру СЗІ за нормативно-правововою, організаційною, інформаційною та іншими складовими; напрямки захисту (*H*), які відображають функціональне призначення; етапи створення (*E*), які формують ступінь забезпечення задач безпеки.

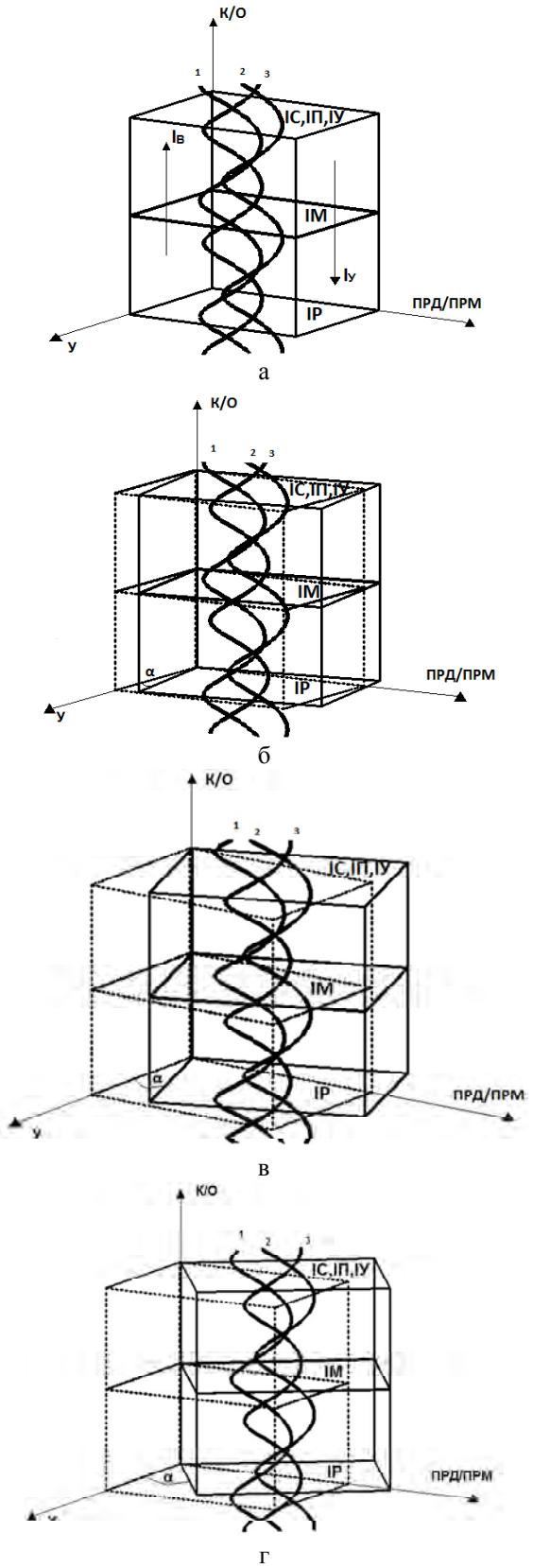

Рис. 3. Модель простору інформаційно-технічних станів БІСК у контексті гарантоздатності:
а – працездатний (безпечний) стан – NORMA;
б – частково працездатний (безпечний) стан – ALARM-1; в – непрацездатний (безпечний) стан – ALARM-2;
г – непрацездатний небезпечний стан – AVARIA

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 (K) визначається таким чином:

$$K = O_i \cdot H_j \cdot E_k ,$$

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)

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

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 багаторівневого захисту БІСК. З метою створення комплексної системи безпеки БІСК у контексті структури гарантоздатності розглянемо модель багаторівневого захисту інформації, яка спрямована на забезпечення інформаційної безпеки на зовнішньому рівні, а також на рівнях апаратно-програмного забезпечення та інформаційних процесів [5] (рис. 4).

Модель системи захисту інформації в БІСК згідно багаторівневої безпеки (рис. 4):

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

де MZ_k^{SVUD} – множина технологій виявлення, блокування (нейтралізації) загроз інформаційній безпеці (S) відповідно до профілів захисту: конфіденційності (V), цілісності (U), доступності (D), яка характерна для кожного з рівнів інформаційної безпеки.

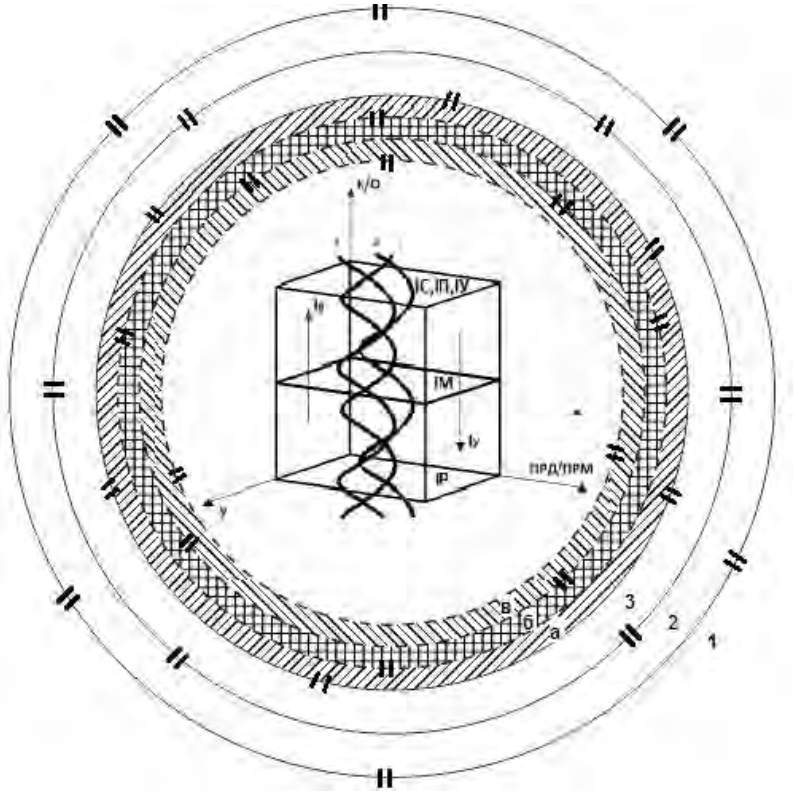

Рис. 4. Модель багаторівневої безпеки БІСК: матричний метод створення СЗІ у сегментах – основи (1), напрями (2), етапи (3): вибір засобів захисту на рівні – зовнішньому(а); апаратно-програмного забезпечення (б); інформаційних процесів (в)

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 шляхом перекривання імовірних каналів НСД та впливів у відповідності до моделі потенційного порушника, що відповідно унеможливлює несанкціоноване ознайомлення з даними, їх модифікацію та знищення за рахунок періодичного контролю блоком управління давачів, що забезпе-

чують виявлення і блокування (нейтралізацію) НСД. Ефект багаторівневого захисту: 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 більше часу життєвого циклу інформації в БІСК та більше часу виявлення і блокування його несанкціонованого доступу.

Загальна міцність трирівневого захисту інформації в БІСК (рис. 4) визначається

$$P_{\Sigma} = 1 - \prod_{i=1}^{m} \left(1 - P_{зi_k}\right),$$

де i = 1...m – номер перепони; m – кількість продубльованих перепон; $P_{зi_k}$ – міцність кожного рівня багатоланкового захисту з контрольованими перепонами, що відповідно визначається

$$P_{зi_k} = P_{зi_{k1}} \cup P_{зi_{k2}} \cup P_{зi_{k3}} \cup ... \cup (1 - P_{обх1}) \cup$$
$$\cup (1 - P_{обх1}) \cup (1 - P_{обх2}) \cup ... \cup (1 - P_{обхj}),$$

де $P_{зi_{kn}}$ – міцність n-ї перепони; $P_{обх\,j}$ – імовірність обходу перепони порушником; j – число шляхів обходу перепони.

Висновки

Розроблено концепцію побудови системи захисту інформації в БІСК, яка є підставою для ефективного її використання у сегментах державної та міжнародної політики інформаційної безпеки в умовах інтелектуалізації суспільства. *Створено* базовий підхід до реалізації СЗІ в БІСК на основі принципів системного аналізу, передбачає вибір оптимальної структури системи захисту та процедуру оцінювання її ефективності. *Адаптовано* модель простору ІТС БІСК згідно структури гарантоздатності за впливу загроз функціональній та інформаційній безпеці. *Розглянуто* інтегральну модель загроз безпеці та модель захищеної БІСК, що уможливлює побудову системи захисту інформації та оцінювання її ефективності матричним методом.

Список літератури

1. Демчук А. Багаторівневі інтелектуальні інформаційні системи опрацювання відеоконтенту для осіб з вадами зору / А. Демчук, Р. Вовнянка, М. Гопяк. – [Електронний ресурс]. – Режим доступу URL: http:// ena.lp.edu.ua:8080/handle/ntb/24831?mode=full.

2. Свистунов В.А. Інтелектуальні системи керування з багаторівневим перетворенням інформації на авіаційному підприємстві / В.А. Свистунов // Авиационно-космическая техника и технология. – 2012. – № 10 (97). – С. 219-222.

3. Сова О.Я. Концепція ієрархічної побудови інтелектуальних систем управління мобільними радіомережами військового призначення / О.Я. Сова, В.А. Романюк, П.В. Жук // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2010. – № 2. – С. 121-130.

4. Бондаренко М. Перспективы применения международного стандарта ISO/IEC 15408 в Украине / М. Бондаренко, Л. Скрыпник, И. Горбенко, А. Потий // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2011. – Вип №3. – С. 7-26.

5. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем / Н.А. Маслова // Штучний інтелект. – 2008. – №4. – С. 253-264.

6. Дудикевич В.Б. Багаторівневі інтелектуальні системи керування: гарантоздатність, безпека об’єктів / В.Б. Дудикевич, Г.В. Микитин, Т.Б. Крет // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 4 (129). – С. 92-95.

7. Dudykevych V.B. The concept of creation of multi-level complex system of cyber-physical systems / V.B. Dudykevych, G.V. Mykytyn, T.B. Kret // Системи обробки інформації. – Х.: ХУ ПС, 2016. – Вип. 5 (142). – С. 87-93.

Надійшла до редколегії 1.06.2016

Рецензент: д-р техн. наук, ст. наук. співр. С.Г. Семенов, Національний технічний університет «ХПІ», Харків.

КОНЦЕПЦИЯ И БАЗОВЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В МНОГОУРОВНЕВОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ УПРАВЛЕНИЯ

В.Б. Дудыкевич, Г.В. Микитин, Т.Б. Крет

Разработана концепция создания системы защиты информации (СЗИ) в многоуровневой интеллектуальной системе управления (МИСУ) на базе структуры “многоуровневая система – многоуровневая защита”. Предложен базовый подход к построению СЗИ в МИСУ на основе принципов системного анализа: архитектура МИСУ – модель угроз, модель информационно-технических состояний системы, модель защищенной МИСУ – структура СЗИ – оценка эффективности СЗИ.

Ключевые слова: *многоуровневая интеллектуальная система, система защиты информации, модель, метод, оценка эффективности.*

THE CONCEPT AND BASIC APPROACH TO BUILDING INFORMATION SECURITY SYSTEM IN MULTI-LEVEL INTELLIGENT CONTROL SYSTEM

V.B. Dudykevych, G.V. Mykytyn, T.B. Kret

The developed concept of creating information security system (ISS) in multilevel intelligent control system (MICS) based on the structure of "multi-level system - multi-level security". Proposed basic approach to building ISS in MICS on the basis principles of system analysis: architecture MICS - threat model, model information-technical state system, model of the protected MICS – structure ISS – evaluation of the effectiveness ISS.

Keywords: *multi-level intelligent system, information security system, model, method, evaluation of effectiveness.*