УДК 004.89

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

Національний університет «Львівська політехніка», Львів

БАГАТОРІВНЕВІ ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ: ГАРАНТОЗДАТНІСТЬ, БЕЗПЕКА ОБ'ЄКТІВ

Розглянуто системний підхід до застосування багаторівневих інтелектуальних систем керування (БІСК) у сфері безпеки об'єктів, який полягає у створенні методологій забезпечення гарантоздатності систем і захищеності інформаційних мереж (ІМ) та побудові структури апаратно-програмної реалізації БІСК безпекою об'єктів. Представлено трирівневу структуру застосування БІСК безпекою об'єктів та проаналізовано один з підходів до її реалізації на основі SCADA-пактів.

Ключові слова: *багаторівнева інтелектуальна система керування, безпека об'єктів, структура гарантоздатності, модель OSI, ресурс реалізації.*

Вступ

Постановка проблеми. Застосування ІСК в різних предметних сферах є одним з головних завдань Національної програми інформатизації та концепції захисту інформації в Україні, виконання якого повинно забезпечувати раціональність та надійність функціонування процесів в умовах невизначеності. Інтелектуальна система керування здатна підтримувати параметри відповідного режиму функціонування, приймати рішення на зміну алгоритму роботи, навчатися в ході досягнення поставленої мети та адаптуватися до зміни зовнішніх умов роботи. Об'єднання ІСК в єдину складну систему обумовлює функціональну багаторівневість її структури. Багаторівневі ІСК створюються для керування складними об'єктами, розподіленням поставлених задач, а також з метою підвищення швидкодії та надійності. У випадку виходу з ладу одного з елементів, його може замінити інший. Багаторівневість не передбачає централізації, що є необхідною умовою надійного функціонування складної системи. Застосування БІСК у сфері безпеки об'єктів дає підстави для підсилення вимог щодо надійності їх функціонування. Прийняття рішення БІСК безпекою об'єкта обумовлене експертними оцінками відповідно до адекватної моделі функціонування об'єкта. З метою ефективного забезпечення функціонування об'єктів у різних предметних сферах, прийняття рішення на управління в умовах невизначеності необхідно:

1) створити методології безпеки БІСК;

2) розробити модель апаратно-програмної реалізації БІСК з врахуванням систем захисту інформації.

Аналіз останніх досліджень та публікацій. Сьогодні активно досліджуються задачі створення теоретичних засад побудови ІСК та вдосконалення технологій їх функціонування [1]. Також дослідження з проблематики застосування ІСК у сфері безпеки об'єктів сьогодні займає одну з головних позицій в межах Рамкової програми "Горизонт-2020", зокрема у сегменті запобігання надзвичайних ситуацій та управління ними у природно-техногенному середовищі.

Мета роботи – створити системний підхід до застосування БІСК у сфері безпеки об'єктів, спрямований на вирішення двох наукових задач: 1) забезпечення гарантоздатності систем та захищеності мереж; 2) розроблення моделі апаратно-програмної реалізації системи керування безпекою об'єктів, що дозволить цілісно забезпечити безпеку структури "БІСК – об'єкт" згідно нормативного забезпечення.

Виклад основного матеріалу

Системний підхід до застосування БІСК у сфері безпеки об'єктів. На рис. 1 представлено трирівневу структуру застосування БІСК у контексті забезпечення безпеки об'єктів в різних предметних сферах: ***безпека БІСК*** **I*:*** методи і засоби забезпечення: функціональної та інформаційної безпеки (1 – структура гарантоздатності); безпеки рівнів інфомаційної мережі (2 – модель OSI); ***безпека об'єктів на основі інтелектуальних давачів БІСК*** **II*:*** 3 – системи керування доступом; 4 – системи радіочастотної ідентифікації; 5 – системи відеоспостереження та сигналізації; 6 – біометричні системи; ***політики безпеки*** застосування БІСК– III.

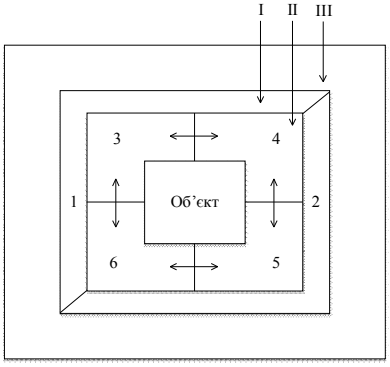

Рис. 1. Системний підхід до застосування БІСК у сфері захисту інформації

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

Безпека БІСК: гарантоздатність систем, захищеність мереж. Трирівнева структура застосування БІСК у сфері безпеки об'єктів дає підстави для обгрунтування критеріїв забезпечення: властивостей гарантоздатності системи, зокрема функціональної та інформаційної безпеки (рис. 2); безпеки окремих рівнів інформаційної мережі згідно моделі OSI (рис. 3), як таких, що забезпечують безпеку БІСК на рівні конфіденційності, цілісності і доступності інформації.

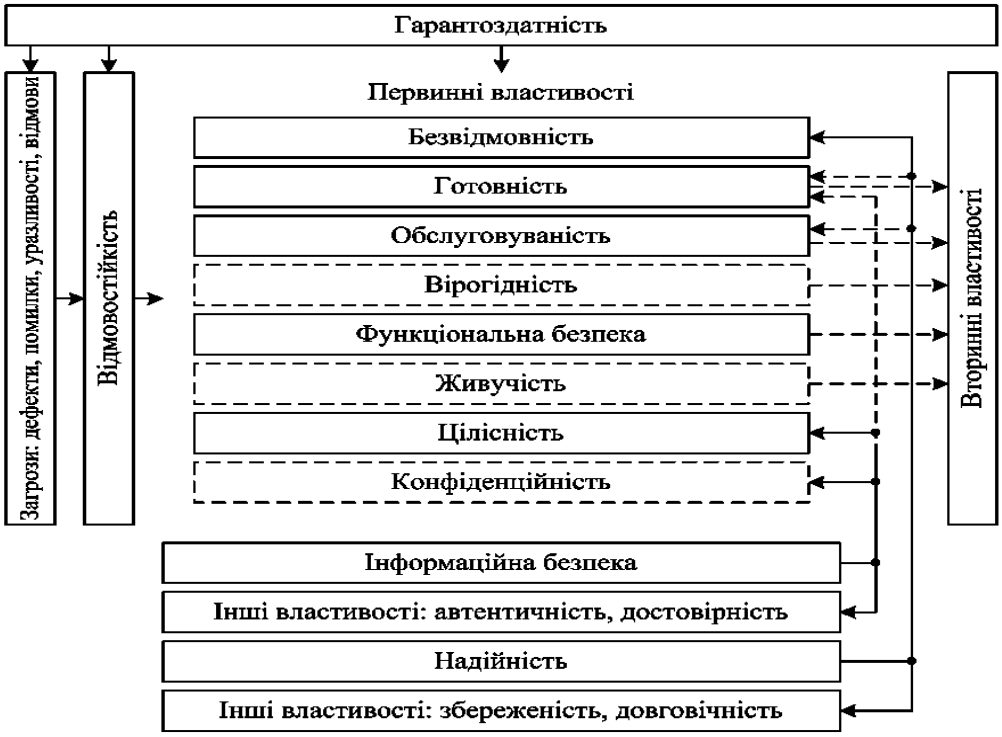

Рис. 2. Структура гарантоздатності: СОУ-Н НКАУ 0060:2010

Модель OSI	
Дані	Рівень
Дані	*Прикладний* доступ до мережевих служб
Дані	*Представлення* представлення і кодування даних
Дані	*Сеансовий* керування сеансом зв'язку
Блоки	*Транспортний* безпечне та надійне з'єднання "точка – точка"
Пакети	*Мережевий* визначення маршруту та IP (логічна адресація)
Кадри	*Канальний* MAC та LLC (фізична адресація)
Біти	*Фізичний* кабель, сигнали, бінарне передавання

Рис. 3. Модель OSI: ДСТУ ISO/IEC 7498-1:2004

Одним з підходів до забезпечення функціональної та інформаційної безпеки БІСК є модель трирівневого багатоланкового захисту, яка є основою для побудови систем безпеки на кожному з рівнів (рис. 4). Одним з підходів до створення системи безпеки ІМ є реалізація захисту інформації на мережевому рівні OSI (табл. 1).

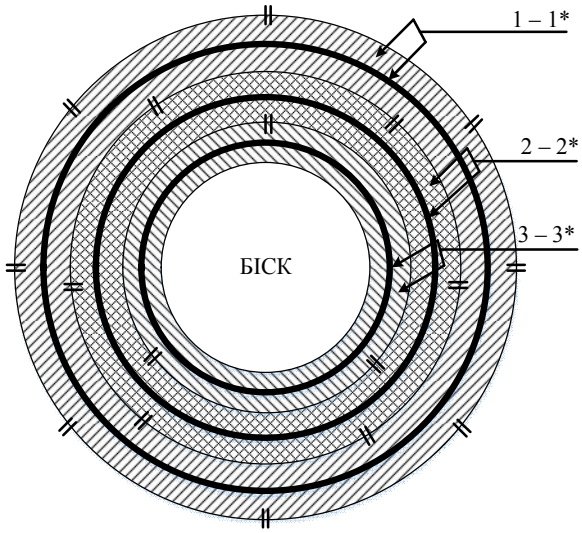

Рис. 4. Модель трирівневого багатоланкового захисту БІСК: – зовнішній рівень ФБ (1) та ІБ (1*); 2 – рівень апаратно-програмного забезпечення ФБ (2) та ІБ (2*); 3 – рівень ФБ (3) та ІБ (3*) інформаційних процесів

Безпека об'єктів: апаратно-прогромний ресурс реалізації БІСК. Апаратно-програмні ресурс автоматизації керування безпекою об'єктів орієнтований на моніторинг зміни стану інтелектуальних давачів контролю та обробку результатів.

Таблиця 1

Безпека БІСК на мережевому рівні

Модель OSI (ДСТУ ISO 7498-2:2004; ДСТУ ISO/IEC 7498-3:2004): **мережевий рівень**	
Топологія	Зірка
Загроза	Відгалуження (програмне або апаратне) трафіку і спрямування його копії на сніффер.
Реалізація загрози	*Dsniff* – набір програм для мережевого аудиту і перевірок на можливість проникнення, які забезпечують: пасивний моніторинг мережі для пошуку потрібних даних; перехоплення мережевого трафіку;, можливість організації MITM-атак для перехоплення сесій SSH і HTTPS за рахунок використання недоліків *Public Key Infrastructure* (інфраструктура відкритих ключів).
Захист	*IPsec (IP Security)* – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжності та/або шифрування IP-пакетів. *IPsec* також містить протоколи для захищеного обміну ключами в мережі Інтернет. *CiscoEasy VPN* – значно спрощує розгортання віртуальних приватних мереж для територіально віддалених офісів і співробітників.

До таких універсальних систем відносяться: OPC сервер; засоби МЕК-програмування контролерів; SCADA-пакети; бази даних.

Стандарт OPC. Стандарт забезпечує можливість спільної роботи засобів автоматизації, що функціонують на різних апаратних платформах, у різних промислових мережах. Після появи стандарту OPC практично всі SCADA – пакети перепроектовані, як OPC – клієнти, а кожен виробник апаратного забезпечення постачає: контролери, модулі вводу-виводу, інтелектуальні давачі і виконавчі пристрої стандартним OPC сервером. В Україні широко використовуються стандарти OPC DA та OPC HDA.

OPC DA сервер. Сервер є найбільш широко використовуваним, призначений для забезпечення обміну даними на рівні клієнтська програма – фізичні пристрої. Дані складаються з трьох полів: "значення", "якість" і "тимчасова мітка". Параметр якості даних дозволяє передати від пристрою клієнтської програми інформацію про вихід вимірюваної (зареєстрованої) величини за рамки динамічного діапазону на рівні: відсутності даних, помилки зв'язку, виявлення загрози. Існує чотири стандартних режими зчитування даних з OPC сервера: синхронний, асинхронний, режим підписки, оновлення даних. У кожному з цих режимів дані можуть зчитуватися з OPC сервера, та безпосередньо з фізичного пристрою. На рис. 5 приведений приклад взаємодії прикладних програм та фізичних пристроїв через OPC сервер [2, 3]. OPC DA сервер має користувальницький інтерфейс, який дозволяє виконувати будь-які допоміжні функції для полегшення роботи з обладнанням. В якості OPC клієнта може виступати програма мовою C ++ (наприклад, SCADA-пакет) або програми іншими мовами (VisualBasic, VBA, Delphi). Програма мовою C ++ взаємодіє з OPC сервером через інтерфейс OPC Custom, а програма на VisualBasic, VBA, Delphi – через інтерфейс автоматизації OPC Automation. OPC сервер і OPC клієнти можуть працювати тільки на комп'ютерах і контролерах з операційними системами, що підтримують технологію DCOM (Windows XP і Windows CE).

OPC сервер підключається до фізичних пристроїв будь-яким способом. Наприклад, сервер NLopc використовує для кожного фізичного пристрою свій драйвер. OPC сервер NLopc є програмною системою, що дозволяє підключити апаратуру, до програмного забезпечення сторонніх виробників, яке задовольняє стандарт OPC. До такого ПЗ належать, зокрема, SCADA-пакети Genesis32, TraceMode, ISaGRAF, InTouch, офісні програми MS Excel, MS Word, програми для автоматизації експерименту LabView, MATLAB т.і.

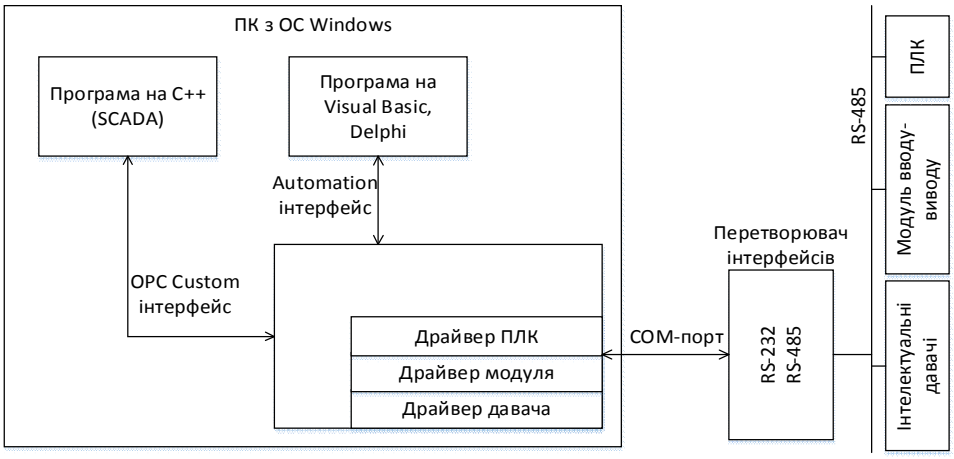

Рис. 5. Апаратно-програмний ресурс реалізації БІСК безпекою об'єктів

SCADA-пакети. Більшість систем автоматизації керування функціонує за участю людини (оператора, диспетчера). Інтерфейс між людиною і системою називають людино-машинним інтерфейсом (ЛМІ). В окремому випадку, коли ЛМІ призначений для взаємодії людини з автоматизованим технологічним процесом, його називають SCADA-системою (Supervisory Control And Data Acquisition) – диспетчерське управління і збір даних. Сучасні SCADA-пакети включають комплекс функцій (рис. 6).

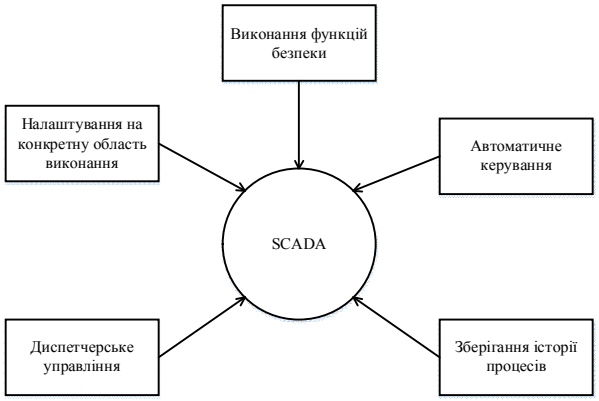

Рис. 6. Функціональна структура SCADA-системи

Бази даних. Система автоматизації керування працює з великими обсягами даних, які необхідно зберігати, сортувати, групувати, витягувати і представляти у вигляді, зручному для користувача. Дані витягуються за допомогою структурованої мови запитів SQL (Structured Query Language). Основними властивостями СКБД є: наявність інтерфейсу користувача на базі мови запитів SQL, можливість одночасного обслуговування декількох користувачів; коректність роботи з даними. Відкриті системи використовують звернення до СКБД через драйвер ODBC (OpenDatabaseConnectivity), який використовується, коли необхідно забезпечити незалежність прикладної програми від типу СКБД і потрібно підключитися до декількох різних СКБД (одночасно до MS SQL Server, MS Excel, MS Access, Paradox т. і.).

Системи програмування на основі МЕК 61131-3. Засоби характеризуються такими показниками: надійністю створюваного програмного забезпечення; можливістю простої модифікації програми і нарощування її функціональності; можливістю повторного використання відпрацьованих фрагментів програми т.і. Серед основних принципів мови МЕК 61131-3 такі: вся програма розбивається на безліч функціональних елементів, кожен з яких може складатися з функцій, функціональних блоків і програм; є засоби для виконання різних фрагментів програми в різний час, з різною швидкістю, а також паралельно; стандарт підтримує структури для опису різнорідних даних; програма, написана для одного контролера, може бути перенесена на інший контролер, сумісний зі стандартом МЕК 61131-3.

Висновок

Системний підхід до застосування БІСК безпекою об’єктів дозволяє створювати підходи до побудови безпеки самих систем і мереж згідно нормативного забезпечення, що у свою чергу, дає підстави для захисту інформації на рівні конфіденційності, цілісності, доступності та забезпечує безпеку об’єктів згідно політики безпеки.

Список літератури

1. Рыбина Г.В. Основы построения интеллектуальных систем / Г.В. Рыбина. – М.: Финансы и статистика, 2010. – 415 с.

2. Соловьев В. Логическое проектирование цифровых систем на основе программируемых логических интегральных схем / В. Соловьев, А. Климович. – М.: Горячая линия – Телеком, 2008. – 376 с.

3. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности / А.Ю. Щербаков. – М.: Издатель Молгачева С.В., 2001. – 352 с.

Надійшла до редколегії 18.02.2015

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

МНОГОУРОВНЕВЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ: ГАРАНТОСПОСОБНОСТЬ, БЕЗОПАСНОСТЬ ОБЪЕКТОВ

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

Рассмотрен системный подход к применению многоуровневых интеллектуальных систем управления (МИСУ) в области безопасности объектов, который заключается в создании методологии обеспечения гарантоспособности систем и защищенности информационных сетей и построения структуры аппаратно-программной реализации МИСУ безопасностью объектов. Представлена трехуровневая структура применения МИСУ безопасностью объектов и проанализирован один из подходов к ее реализации на базе SCADA-пактов.

Ключевые слова: *многоуровневая интеллектуальная система управления, безопасность объектов, структура гарантоспособности, модель OSI, ресурс реализации.*

MULTI-LEVEL INTELLIGENT CONTROL SYSTEMS: GUARANTEED RELIABILITY, SECURITY FACILITIES

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

Investigated a systematic approach to the use of multi-level intelligent control systems in the field of security objects. Depicted principle and methodology of guaranteed reliability and security information network. The structure created of hardware and software implementation multi-level intelligent control systems security facilities. Presented by the three-tier structure of multi-level intelligent control systems of the security objects and analyzed one of the approaches to their the implementation of SCADA-based.

Keywords: *multi-level intelligent control system, security facilities, structure guaranteed reliability, model OSI.*