УДК 004.89, 004.056

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

КОМУНІКАЦІЙНЕ СЕРЕДОВИЩЕ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ КЕРУВАННЯ: БАГАТОРІВНЕВІСТЬ ТА ЗАХИСТ ІНФОРМАЦІЇ

Розглянуто проблему забезпечення взаємозв’язку між окремими інтелектуальними системами, які здійснюють управління певним об’єктом (пристрій, система). Досліджено об’єднання інтелектуальних систем між собою, що вносить функціональну багаторівневість у середовище комунікації. Проаналізовано загрози, які можуть виникнути під час роботи, та методи запобігання цим загрозам.

Ключові слова: інтелектуальна система керування, комунікаційне середовище, багаторівневість, захист інформації.

The problem of the relationship between individual intelligent systems that manage the particular entity (a device, system) has bee reviewed. Investigated associations of intellectual systems have been studied, which introduces functional multi-level in the environment of communication. Threats that may arise during the work and troubleshooting methods have been analyzed.

Key words: intelligent control system, communication environment, multi-level, information security.

Вступ

Інтелектуальна система (ІС) є самокерованою кібернетичною системою, яка оперує знаннями в певній предметній області та здатна на основі безпосереднього сприйняття і подальшого аналізу поточної ситуації планувати дії, спрямовані на досягнення певної мети, а також поповнювати свої знання. До предметних областей, в яких використовують ІС, належать: інтерпретація, прогнозування, діагностика, проектування, планування, моніторинг, налагодження, ремонт, навчання, керування. Процес керування передбачає вирішення завдань інтерпретації, прогнозування, ремонту, моніторингу системи тощо. Застосування *інтелектуальних систем керування* (ІСК) знаходять в найрізноманітніших галузях (промисловість, будівництво, транспорт, ракетобудування тощо). Зважаючи на вирішувані завдання та області застосування ІСК, посилюється актуальність їх дослідження.

Важливим фактором роботи ІСК є взаємозв’язок між собою, а також з іншими системами керування. Застосування інформаційно-комунікаційних мереж дозволяє здійснити взаємоузгоджене функціонування програмних та програмно-апаратних компонентів ІСК. Забезпечення захищеного передавання даних та інформації, враховуючи застосування цих систем керування, висуває високі вимоги як до будови та функціонування ІСК, так і до інформаційно-комунікаційної мережі.

Аналіз останніх досліджень та публікацій

У роботах [1] розглянуто широке коло завдань, що здатні вирішувати кіберфізичні системи. Досліджуються підходи до розроблення ІС, наповнення баз знань та їх адаптації до предметної області застосування. Окреслюються ІСК як складові кібернетичних систем, особливості їх побудови та функціонування.

Робота [2] доводить практичне застосування ІС у технології інтелектуального збирання даних у кіберфізичних системах. Зображено узагальнену функціональну схему автономного агента та багато-агентну систему, які слугують як програмним забезпеченням для систем керування з інтелектуальними характеристиками. Актуальність досліджень, пов’язаних з ІСК, подано в роботі [3], де визначено ІСК як программно-апаратний засіб на основі систем штучного інтелекту, подано основні завдання, які вирішують ці системи.

Зважаючи на сфери застосування ІСК, актуальним є питання захищеності даних та інформації, що циркулює в них. Деякі аспекти захисту інформації в ІСК, а також блок-схему атаки на ІСК було визначено в роботах [4]. Велику увагу приділено потенційним уразливостям, присутність яких може слугувати загрозою системі, яка функціонально є багаторівневою. Окреслені вразливості показують не повний спектр захисту мережевого середовища, тому доцільно проаналізувати цей сегмент ІСК.

Мета роботи

Метою статті є дослідження мережевого сегменту багаторівневої моделі як комунікаційного середовища та забезпечення ефективності його захисту для ІСК.

Основна частина

Розглянемо ІСК як складну, автоматичну, адаптивну, самонавчальну та автономну мережу із взаємопов'язаних між собою інтелектуальних давачів (сенсорів), які здатні аналізувати отриману інформацію, робити умовиводи для вирішення поставленої задачі та здійснювати процес керування. Об'єднання частин ІСК в єдину систему зумовлює функціональну багаторівневість та масштабованість, яка допомагає керувати складними об'єктами, розподіляти необхідні задачі, що, своєю чергою, підвищує швидкодію та надійність. Масштабованість мережі залежить від вирішуваних завдань та лежить у межах від одиниць до десятків тисяч. Надійність функціонування ІСК слід розглядати в контексті гарантоздатності.

Функціональну багаторівневість ІСК можна визначити за п'ятьма рівнями:

1-й рівень утворюється з інтелектуальних давачів (вузли системи), які є стандартизованими для певної технології та здатні працювати автоматично, автономно, здійснювати самонавчання та адаптацію алгоритму під час роботи. Інтелектуальні давачі розташовуються у випадковій послідовності, що залежить від фактору виконуваних задач та середовища функціонування, в якому розміщено об'єкт керування;

2-й рівень – комунікаційне устаткування (фізичні носії інформації, різні мережеві адаптери, повторювачі, концентратори, маршрутизатори тощо);

3-й рівень – операційні системи, для забезпечення та створення програмної платформи мережі ІСК, налагодження її функціонування;

4-й рівень – мережеві засоби (мережеві бази даних, поштові системи, засоби архівування даних);

5-й рівень – виконавчі пристрої.

Топології мережевого сегменту ІСК. Побудова ІСК передбачає застосування топології, тобто способу організації фізичних зв'язків між її елементами. Розглянемо топології, на основі яких можуть будуватися ІСК:

Повнозв'язна топологія – кожний вузол пов'язаний з усіма іншими (рис. 1, *а*).

Комірчаста топологія – вилучення деяких можливих зв'язків з повнозв'язної топології (рис. 1, *б*).

Загальна шина – усі елементи з'єднуються через єдину шину (магістраль) (рис. 1, *в*).

Топологія зірка – кожен вузол під'єднується до концентратора, який здійснює комутацію (рис. 1, *г*).

Ієрархічна топологія – топологія мережі, де об'єднуються декілька топологій типу зірка за допомогою концентраторів (рис. 1, *д*).

Кільцева топологія – дані передаються від одного вузла до іншого, зазвичай в одному напрямку (рис. 1, *е*).

Зважаючи на неоднорідність середовища, в якому будується ІСК доцільним буде використання комірчасту та ієрархічної топології (рис. 1, *д*). Вузли такого типу мереж розташовуються в довільному порядку. Кожен вузол може здійснювати збирання даних і визначати маршрут передавання до кінцевого виконавчого пристрою. Під час ретрансляції даних вузлом мережі працює, як маршрутизатор, а під час передавання в інший сегмент – як координатор.

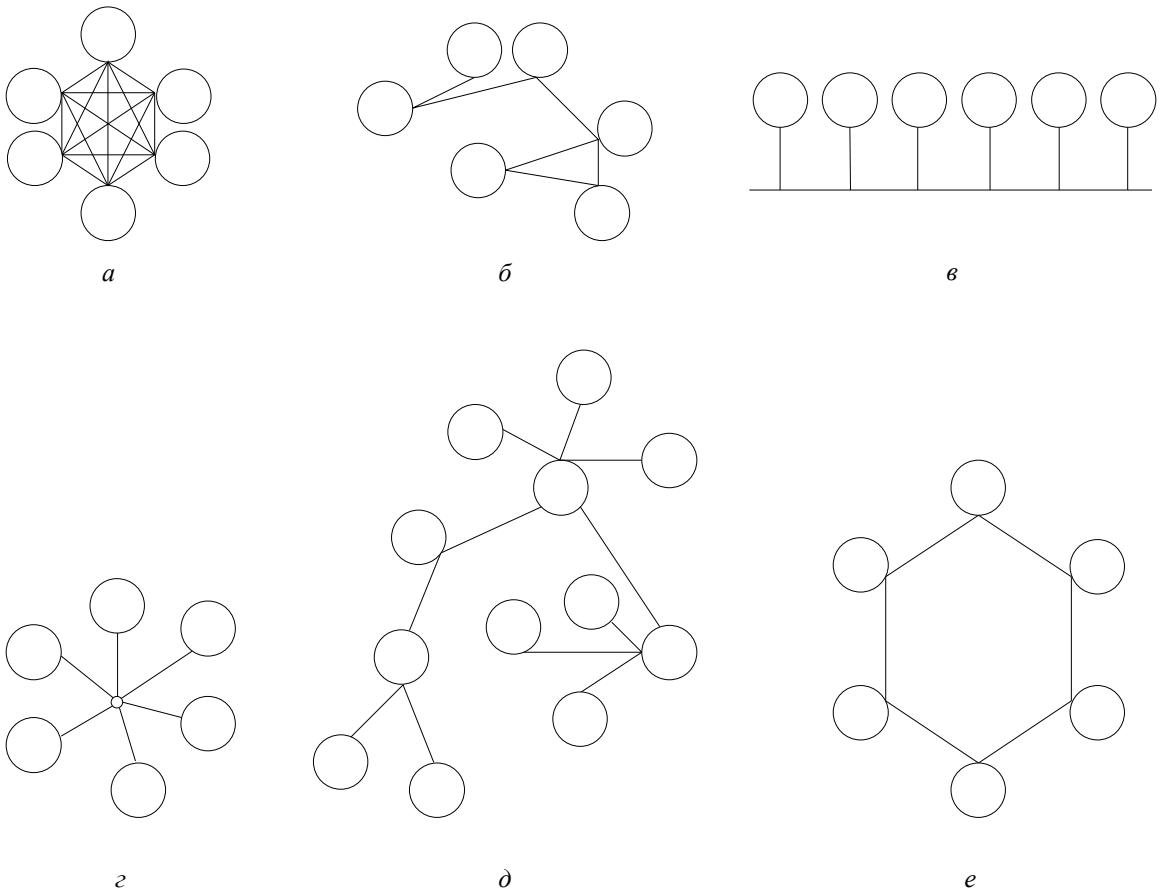

Рис. 1. Топології побудови ІСК

Для спрощення комунікації застосовується абстрактна мережева модель взаємодії відкритих систем (OSI), яка слугує основою розроблення мережевих протоколів. Модель OSI визначає рівні взаємодії систем, задає стандартні імена і вказує, які функції має виконувати кожен рівень.

Технології (KNX/EIB, LonWorks, BACnet, ZigBee), що дають змогу будувати ІСК, можна розглянути на основі мережевої моделі OSI. Представляють децентралізовані мережі, підтримують стандартні протоколи передачі даних, які реалізуються різними засобами комунікації.

Класифікація атак на мережевий сегмент ІСК. Зважаючи на ієрархічні топології та модель взаємодії OSI, що застосовуються для побудови ІСК, уразливості матимуть спільний характер з тими, які виникають у комп'ютерних мережах та можуть спричинити виникнення двох типів атак (пасивних та активних).

Пасивні атаки – спрямовані на прослуховування, моніторинг, перехоплення даних. Зловмисник обмежується отриманням змісту повідомлення, але не модифікує самого повідомлення. У цьому випадку виявити зловмисника дуже важко, а найкращим захистом є профілактика цього типу загрози виконанням дій з шифрування, зміни паролів відповідно до політики безпеки. До пасивних типів атак належать: аналіз трафіку (sniffing), викрадення паролів, сканування мережі, соціальна інженерія.

Активні атаки – на відміну від пасивних, зловмисник під час такої атаки модифікує дані або ж підмінює їх, перериває передачу тощо. Зважаючи на сфери застосування ІСК, це може призвести до значних збитків. Існує кілька типів таких атак:

- маскарад (masquerade) – зловмисник імітує події, які відбуваються в ІСК, створюючи ілюзію коректного функціонування системи;
- повторення (replay) – атака шляхом запису і повторного відтворення автентифікаційних даних, які було введено в систему легітимним пристроєм (користувачем);
- модифікація (modification) – зміна оригінальних даних та інформації;
- відмова в обслуговуванні (denial of service) полягає у насиченні мережевого трафіку до вузла та переповненні буферу, що призводить до відмови у доступі.

Протидія пасивним та активним атакам полягатиме у застосуванні множини заходів для конкретної ІСК та реалізованої топології. На основі аналізу конкретних ситуацій розглянемо заходи запобігання атакам [5]:

1) запобігання виникненню умов, що сприяють появі факторів дестабілізації;
2) запобігання уразливостям, які виникали в минулому;
3) виявлення уразливостей, що проявилися;
4) попередження впливу факторів дестабілізації на систему;
5) виявлення дії факторів дестабілізації на ІСК;
6) локалізація атаки на систему;
7) ліквідація наслідків, що призвели до атаки (уразливостей та дестабілізуючих факторів).

З математичного погляду запобігання атакам є сумою ймовірностей застосування вищезазначених заходів. Забезпечення ефективного захисту пов'язане з ресурсами, затраченими на його реалізацію, тому рівень здійснення захисту, за інших однакових умов, відповідатиме кількості ресурсів.

ZigBee – комунікаційне середовище для ІСК. Ця технологія дає змогу здійснювати бездротове передавання даних, здійснює самоорганізацію та здатна до самовідновлення. З цього погляду застосування цієї технології є актуальним для побудови мережевого сегменту ІСК. ZigBee використовує три типи пристроїв: координатор, маршрутизатор та кінцевий пристрій (здійснює комунікацію із вузлами вищого рівня). Зважаючи на мале енергоспоживання модулів ZigBee, їх застосовують як вбудовані додатки.

З погляду захисту інформації ZigBee передбачає використання 128-бітного ключа для реалізації механізмів безпеки, що грунтується на 128-бітному AES алгоритмі. Застосовується три типи ключів: головний, мережевий та ключ каналів зв'язку. Підтримується як стандартний, так і підвищений режими безпеки.

Висновки

Розглянуто проблему забезпечення взаємозв'язку між окремими інтелектуальними системами, що здійснюють керування певним об'єктом (пристрій, система). Основна функція, яка покладається на комунікаційне середовище, полягає в швидкому та надійному обміні даними та інформацією між окремими інтелектуальними системами керування. Показником ефективності цього комунікаційного середовища є максимальний обсяг інформації, який можна надійно передати за мінімальний час. Цей показник залежить від: пропускної здатності, структури, способу з'єднання тощо. Характеристики перелічених особливостей було використано в роботі для вибору оптимальної комунікації. Досліджено об'єднання інтелектуальних систем між собою, що вносить функціональну багаторівневість у середовище комунікації. Запропоновано модель багаторівневої взаємодії, що дає змогу створювати багаторівневі інтелектуальні системи керування. Проаналізовано загрози, що можуть виникнути під час роботи та шляхи їх протидії. Для побудови комунікаційних зв'язків між окремим давачами ІСК запропоновано використовувати технологію ZigBee.

1. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку / А. О. Мельник // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – 2014. – № 806. – С. 154–161. 2. Матеріали Першого наукового семінару: "Кіберфізичні системи досягнення та виклики". – Львів: НВФ "Українські технології", 2015. – 178 с. 3. Крет Т. Системи керування з інтелектуальними характеристиками / Т. Крет, В. Дудикевич // Комп'ютерні технології друкарства. – 2014. – № 31. – С. 26–29. 4. Крет Т. Б. Захист інформації в інтелектуальних системах керування / Т. Б. Крет // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – 2014. – № 806. – С. 119–123. 5. Бабак В. П. Теоретичні основи захисту інформації: підручник / В. П. Бабак. – К.: Кн. вид-во НАУ, 2008. – 750 с.