УДК 004.89, 004.056

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

ЗАХИСТ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КЕРУВАННЯ

Розглянуто системи керування, які характеризуються наявністю механізму системного оброблення знань. Встановлено способи створення інтелектуальних систем керування, проаналізовано їх захищеність на випадок ймовірних атак. Запропоновано інформаційну модель багатоланкової безпеки багаторівневих інтелектуальних систем керування.

Ключові слова: інтелектуальні системи керування, загрози безпеки, захист інформації.

INFORMATION PROTECTION IN INTELLECTUAL CONTROLLING SYSTEMS

The paper considers intelligent control systems, examines the state of their security during the probable attacks. Describes methods of protecting information systems. The proposed information model multi-tier security in multi-level intelligent control systems.

Key words: intelligent control systems, threats to security, information security.

Вступ

Системи керування (СК) за останні роки зазнали значних змін, все частіше їх будують на основі нових алгоритмів оброблення інформації, а їх апаратна реалізація набула значного поширення. Змінам, яких зазнали СК, значною мірою сприяло вдосконалення та наукові дослідження нейронних мереж, генетичних алгоритмів, систем підтримки-прийняття рішень, нечіткої логіки, експертних систем. На їх основі створюються новітні апаратно-програмні комплекси. СК стають інтелектуальнішими, характеризуються швидкістю та якістю керування, зменшується безпосередня участь людини в цьому процесі. Ці переваги роблять інтелектуальні СК (ІСК) надзвичайно поширеними.

Сфера використання ІСК ставить значно вищі вимоги до них з погляду безпеки та захисту інформації, на відміну від інших СК. Це зумовлено кількістю загроз, яким можуть піддаватися ІСК, та збитками у разі їх некоректного функціонування. Дотримання вимог до системи захисту інформації (СЗІ) необхідне на всіх життєвих циклах в ІСК: “проектування – виготовлення – встановлення – експлуатація”. На практиці вимоги до СТЗ упродовж життєвого циклу ІСК не завжди забезпечуються, що призводить до загрози безпеки людини, суспільства та держави загалом [1].

Виникає проблема захисту інформації в ІСК, для вирішення якої існує як спільний для всіх ІСК метод розв’язання, так і пов'язаний з конкретною системою [2]. Цілком виправданою необхідністю є усунення уразливостей недосконалого проектування систем та обладнання, що застосовується в ІСК, дослідження їх характеристик та ефективності з погляду безпеки.

Інтелектуальна система керування: узагальнена структура, класи загроз

Інтелектуальна система керування. Вчені в галузі автоматики та управління дають таке визначення ІСК – це СК, здатна до “розуміння” і навчання щодо об'єкта керування, зовнішнього

середовища та умов роботи [3, 4]. Основною відмінністю ІСК від інших СК є наявність механізму системного оброблення знань, що може бути доповнений засобами самонавчання на основі накопиченого досвіду [5]. До технологій, що дають змогу створювати ІСК, належать: еволюційні методи і генетичні алгоритми, штучні нейронні мережі, нечітка логіка, експертні системи [6]. Застосування ІСК є надзвичайно широким та залежить від завдань, які вирішуються: діагностика, моніторинг, прогнозування, проектування, навчання, підтримка прийняття рішень тощо.

Поширюється застосування ІСК для моніторингу надзвичайних ситуацій [7, 8, 9]. Проте уразливості з погляду захисту інформації, які спостерігаються протягом циклу “проектування – виготовлення – встановлення – експлуатація”, не забезпечують потрібного рівня безпеки та можуть слугувати для проникнення в систему.

Узагальнена структура ІСК. В ІСК основною архітектурною особливістю, що відрізняє їх від інших СК, є наявність механізму зберігання та обробки знань, для виконання необхідних функцій в невизначених умовах за випадкового впливу зовнішніх ознак [5]. До таких впливів можуть належати непередбачувані зміни цілей, експлуатаційних характеристик системи та об’єкта керування, параметрів зовнішнього середовища (рис. 1). Також склад ІСК за необхідності можна доповнити засобами самонавчання.

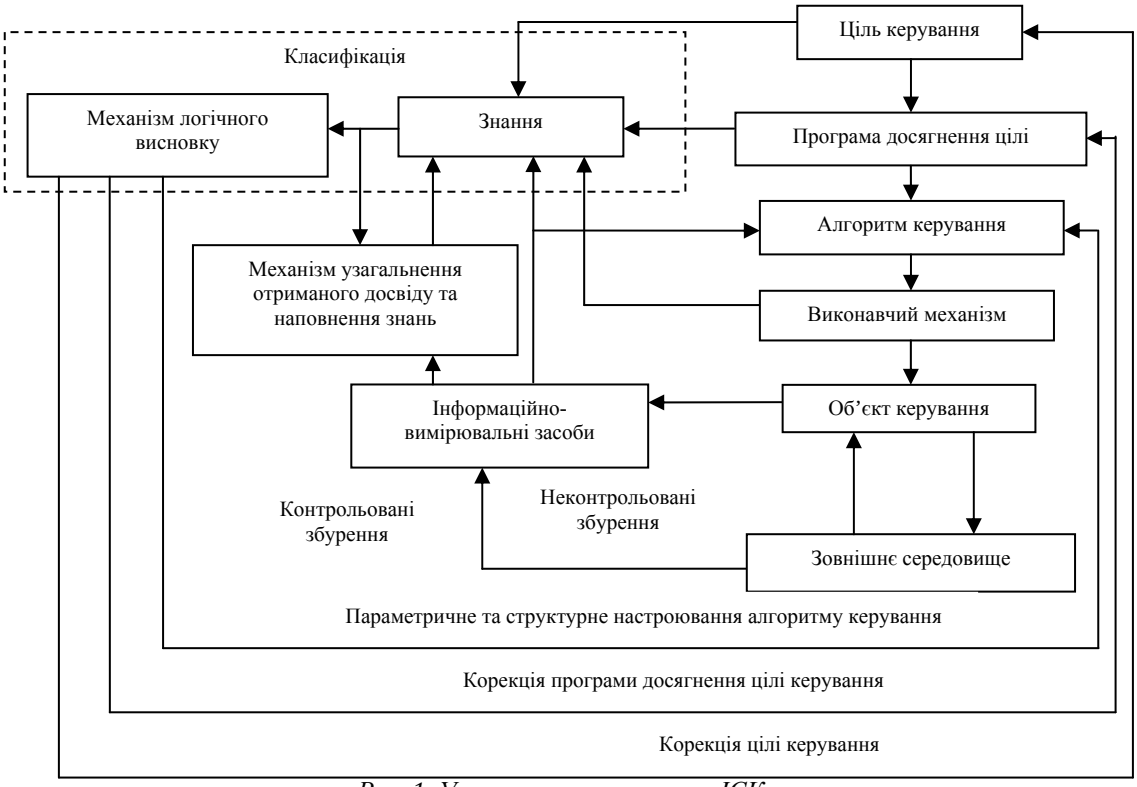

Рис. 1. Узагальнена структура ІСК

У загальному випадку об’єкт керування може мати достатньо складну конструкцію, з низкою функціонально підконтрольних систем. Це зумовлює багаторівневу структуру системи керування. Багаторівневі ІСК (БІСК) характеризуються інтелектуальними можливостями розпізнавання та аналізу, формування стратегії поведінки, послідовність виконання дій, а також синтезу виконавчих алгоритмів.

Класи загроз. Визначення можливих уразливостей в ІСК є ключовим етапом для забезпечення “цілісності–доступності–конфіденційності” (рис. 2). ІСК складаються з різних пристроїв, з’єднаних у єдину мережу. Несанкціонований доступ зловмисника до пристроїв та вузлів ІСК можна реалізувати маніпулюванням функціями керування пристроїв та перехопленням даних, якими обмінюються пристрої у мережі.

Сенсори, актуатори, контролери об’єднують в мережу. Для обміну даними з пристроями інших мереж їх з’єднують у магістраль. Пристрої керування під’єднують до магістралі, вони

слугують для конфігурування, обслуговування, оперативного реагування. Доступ до ІСК може здійснюватися віддалено з ноутбуків, смартфонів чи телефонів. Мережеві пристрої можуть обмінюватися даними через радіоканал.

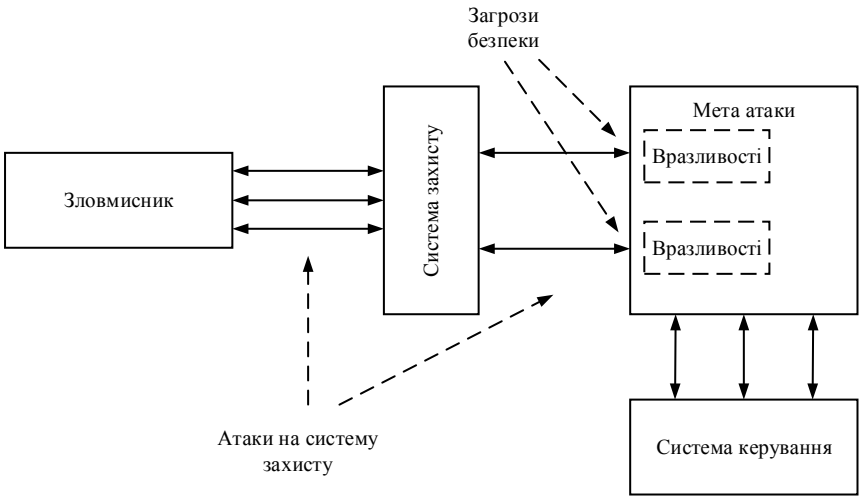

Рис. 2. Блок-схема атаки на ІСК

Можна виділити п’ять потенційних уразливостей, що можуть використовуватись для атаки на ІСК, а саме мережеві, магістральні, комутаційні уразливості мережевих пристроїв та пристроїв керування:

- зловмисник може отримати доступ до даних, якими обмінюються мережеві пристрої (атака на мережу);
- дані, що передаються по магістралі, можуть бути перехоплені чи видозмінені, зловмисник отримає інформацію про структуру ІСК та кількість обладнання (атака на магістраль);
- перехоплення трафіку, що проходить через комутатори, та відкриття доступу до мережі через Інтернет (атака на комутатор);
- зміна конфігурації, алгоритму роботи самих мережевих пристроїв, що призведе до маніпуляції пристроями (атака на мережеві пристрої);
- втручання в роботу пристроїв керування (атака на пристрої керування).

Такі загрози можна зарахувати до двох класів – на рівні мережі та на рівні пристроїв [10]. Для здійснення атаки на мережу противнику необхідно мати фізичний доступ до неї, що легко досягається з використанням радіодіапазону для обміну даними. Таку атаку можна реалізувати через мережевий інтерфейс іншого пристрою. Атаки на пристрій здійснюються через уразливості самого програмного забезпечення, фізичне втручання, збір інформації про роботу пристрою. Оскільки уразливості пристроїв не можна розглядати як такі, що можуть впливати на функціонування усієї ІСК, то на практиці зосереджуються на уразливостях мережі та формуванні підходів до її захисту.

Системна модель багаторівневої ІСК надзвичайними ситуаціями: багатоланковий захист

Системна модель багаторівневої ІСК. У контексті запобігання надзвичайним ситуаціям техногенного, природного, техногенно-природного характеру актуальним є питання створення багаторівневих ІСК, які на основі збору/відбору інформації про стан досліджуваних об’єктів дають підстави для прийняття рішення з керування надзвичайними ситуаціями (рис. 3). Така модель дасть змогу створювати повноінформативну базу знань у сфері запобігання надзвичайним ситуаціям, приймати рішення щодо керування техногенними і природними об’єктами та коригувати політику інформаційної безпеки держави.

Багатоланковий захист інформації в БІСК. Функціонування інтелектуальних систем керування повинно бути безпечним [11]. Розглянемо багатоланковий захист БІСК згідно з

концептуальним підходом до побудови безпеки автоматизованої системи відповідно до моделі порушника (рис. 4). Прикладом такого виду захисту може бути приміщення, в якому встановлена БІСК. Перепонами різної міцності вважаються: стіни, стеля, підлога, вікна і замок на двері.

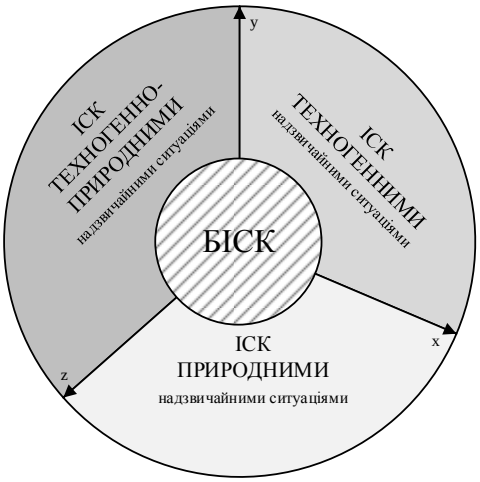

Рис. 3. Системна модель БІСК у сфері надзвичайних ситуацій

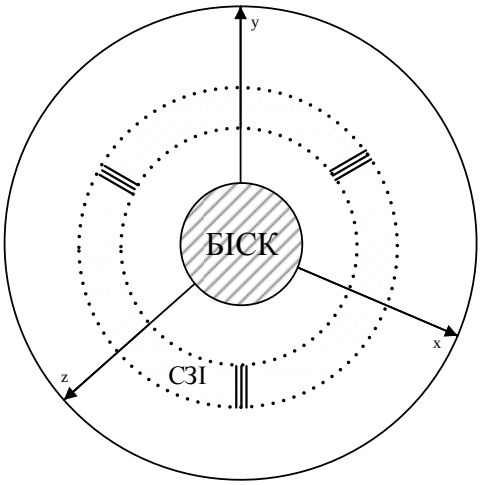

Рис. 4. Інформаційна модель багатоланкового захисту БІСК

Наприклад, система контролю відкриття апаратури і система розпізнавання та розмежування доступу, що контролюють доступ до БІСК, утворюють замкнений захисний контур. До захисного контуру на рівні ланок увійдуть: системи контролю доступу в приміщення; засоби захисту від побічного електромагнітного випромінювання; засоби шифрування.

Розглянемо аналіз перепони у вигляді автоматизованої системи виявлення і блокування несанкціонованого доступу (НСД), де необхідно враховувати надійність її функціонування і шляхи можливого обходу її порушником.

Імовірність відмови системи визначають за відомою формулою

$$P_{від}(t) = e^{-\lambda t}, \quad (1)$$

де λ – інтенсивність відмов групи технічних засобів, що становлять систему виявлення і блокування НСД; t – інтервал часу функціонування системи виявлення і блокування НСД, що розглядається.

З урахуванням можливої відмови системи контролю міцність перепони визначають за формулою

$$P_{зі_k} = P_{вбл}(1 - P_{від}) \cup (1 - P_{обх_1}) \cup (1 - P_{обх_2}) \cup ... \cup (1 - P_{обх_j}), \quad (2)$$

де $P_{вбл}$ і $P_{від}$ визначають відповідно за формулами

$$P_{вбл} = \frac{t_п}{T_{вбл}} \text{ та } P_{від}(t) = e^{-\lambda t},$$

де $T_{вбл}$ – час виявлення і блокування несанкціонованого доступу; $t_п$ – очікуваний час подолання перепони порушником.

$P_{від}$ і кількість шляхів обходу j визначають експертно на основі аналізу принципів побудови системи контролю і блокування НСД.

Тоді вираз для міцності багатоланкового захисту з використанням неконтрольованих перепон можна подати у вигляді:

$$P_{зі} = P_{зі_1} \cup P_{зі_2} \cup P_{зі_3} \cup ... \cup P_{зі_i} \cup (1 - P_{обх_1}) \cup (1 - P_{обх_2}) \cup ... \cup (1 - P_{обх_j}), \quad (3)$$

де $P_{зі_i}$ – міцність *і*-ї перепони.

Вираз для міцності багатоланкового захисту з контрольованими перепонами буде таким:

$$P_{зі_k} = P_{зі_{k1}} \cup P_{зі_{k2}} \cup P_{зі_{k3}} \cup ... \cup P_{зі_{ni}} \cup (1 - P_{обх_1}) \cup (1 - P_{обх_2}) \cup ... \cup (1 - P_{обх_j}), \quad (4)$$

де $P_{зі_{kn}}$ – міцність *n*-ї перепони.

Висновки

Проаналізовано узагальнену структуру ІСК та ймовірні загрози. Запропоновано системну модель багаторівневої ІСК надзвичайними ситуаціями. Створено інформаційну модель багатоланкової безпеки багаторівневих ІСК, що дає підстави для обґрунтування вибору систем захисту інформації відповідно до моделі порушника та комплексу загроз.

1. Закон України "Про основи національної безпеки України" від 19.06.2003 р. № 964-IV. 2. Дудикевич В. Б. Аналіз безпеки багаторівневих інтелектуальних систем керування / В. Б. Дудикевич, Т. Б. Крет // Тези доповідей VI міжнародної НПК "Проблеми і перспективи розвитку IT-індустрії". – Харків, 17–18 квітня 2014 р. – Т. 2. – С. 249. 3. Усков А. А., Круглов В. В. Интеллектуальные системы управления на основе методов нечеткой логики. – Смоленск: Смоленская городская типография, 2003. – 177 с. 4. Апостолюк В. О., Апостолюк О. С. Інтелектуальні системи керування: конспект лекцій. – К.: НТУУ "КПІ", 2008. – 88 с. 5. Искусственный интеллект и интеллектуальные системы управления / Макаров И. М., Лохин В. М., Манько С. В. – М.: Наука, 2006. – 333 с. 6. Дудикевич В. Б. До питання функціональної безпеки інтелектуальних систем керування / В. Б. Дудикевич, Г. В. Микитин, Т. Б. Крет // матер. III міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем". – Львів, 5–6 червня 2014 р. – С. 62. 7. Гурник А. В. Застосування інтелектуальної сенсорної техніки для моніторингу та пошуково-рятувальних робіт / А. В. Гурник, С. В. Валуйський // Східно-європейський журнал передових технологій. – 2013. – Вип. 3/9(63). – С. 1–12. 8. Лобанчикова Н. М. Моделі та методи побудови автоматизованої системи виявлення та попередження надзвичайних ситуацій на території аеропорту: автореф. дис. канд. техн. наук: 05.13.06 / Херсон. нац. техн. ун-т. – Херсон, 2010. – 20 с. 9. Юхимчук С. В. Використання інтелектуальних технологій для аналізу небезпечних ситуацій на залізничному транспорті / С. В. Юхимчук, Т. О. Савчук, М. Д. Кацман // Систем. дослідж. та інформ. технології. – 2009. – № 4. – С. 53–60. 10. Granzer W. Secure Communication in Home and Building Automation Systems: dissertation. – Wien, 2010. – 210 p. 11. Мельников В. В. Безопасность информации в автоматизированных системах: монография / В. В. Мельников. – М.: Финансы и статистика, 2003. – 367 с.