УДК 004.032.2

О. З. Шологон
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ВИДИ ЗАГРОЗ У КІБЕРФІЗИЧНИХ СИСТЕМАХ

Проаналізовано різновиди атак та властивості безпечності у кіберфізичних системах. Для забезпечення збереження конфіденційності та захисту цілісності інформації розглянуто вимоги щодо криптографічних засобів захисту інформації у складі КФС.

Ключові слова: кіберфізичні системи, атаки, криптографія

THREADS TYPES IN CYBER PHYSICAL SYSTEMS

In the paper types of attacks and security properties of cyber-physical systems analysed. Requirements to cryptographical units for data security in cyber-physical system are reviewed to ensure the confidentiality and integrity of information.

Key words: cyber-physical systems, attacks, cryptography.

Вступ

Захист інформації завжди викликав зацікавлення, і в наш час, коли комп’ютерні технології використовуються у більшості сфер нашого життя, безпека є важливішою, ніж будь-коли.

Термін “кіберфізичні системи” визначає системи, які забезпечують взаємодію між реальним світом та інформаційними системами. Основною метою кіберфізичних систем є контроль поведінки фізичних об’єктів, частиною яких вони є. КФС не є традиційними системами у режимі реального часу, вони надають додаткові властивості класичним системам. Їх кібер- і фізичні компоненти інтегровані для навчання та адаптації, самоорганізації та продуктивності.

Огляд літератури

У наш час головною проблемою стає надійна взаємодія систем управління з фізичними системами [1]. Інформаційні системи з кожним днем стають все складнішими і тому найменший витік інформації може стати фатальним [9]. У зв’язку з цим сучасні дослідження спрямовані на створення систем, які б змогли збалансувати поєднання фізичних і обчислювальних елементів [4]. Такі системи називаються кіберфізичними системами (КФС) [2].

Загалом відомо багато методів забезпечення безпеки (аутентифікація, контроль доступу, цілісність повідомлень) [3]. Однак вони спрямовані більше на захист інформації, а не фізичних систем [5]. На практиці ці методи можуть бути зруйновані через людські помилки, неточності програмного забезпечення, збої у налаштуванні пристроїв [7]. Наслідком цього можуть бути успішні атаки зловмисників на КФС [8]. Захист даних за допомогою шифрування – одне з можливих вирішень проблеми безпеки [6]. Зашифрований текст стає доступним тільки для того, хто знає секретний ключ [10]. Цим питанням займається криптографія [11]. Все ще немає чітких вимог щодо криптографічного захисту інформації, тому в статті будуть сформульовані властивості, якими має володіти КФС, щоб бути надійною [12].

Мета роботи

Метою роботи є узагальнення видів атак та загроз у кіберфізичних системах, а також формулювання криптографічних вимог до КФС.

Характеристики КФС

Основним завданням кіберфізичних систем є контроль поведінки фізичного об’єкта, частиною якого вони є, а також можливіть зміни поведінки системи за необхідності.

Кіберфізичні системи застосовують у багатьох сферах, таких як управління охороною здоров’я, автомобільне управління, електромережі, фізична інфраструктура (дороги, мости) (рис. 1).

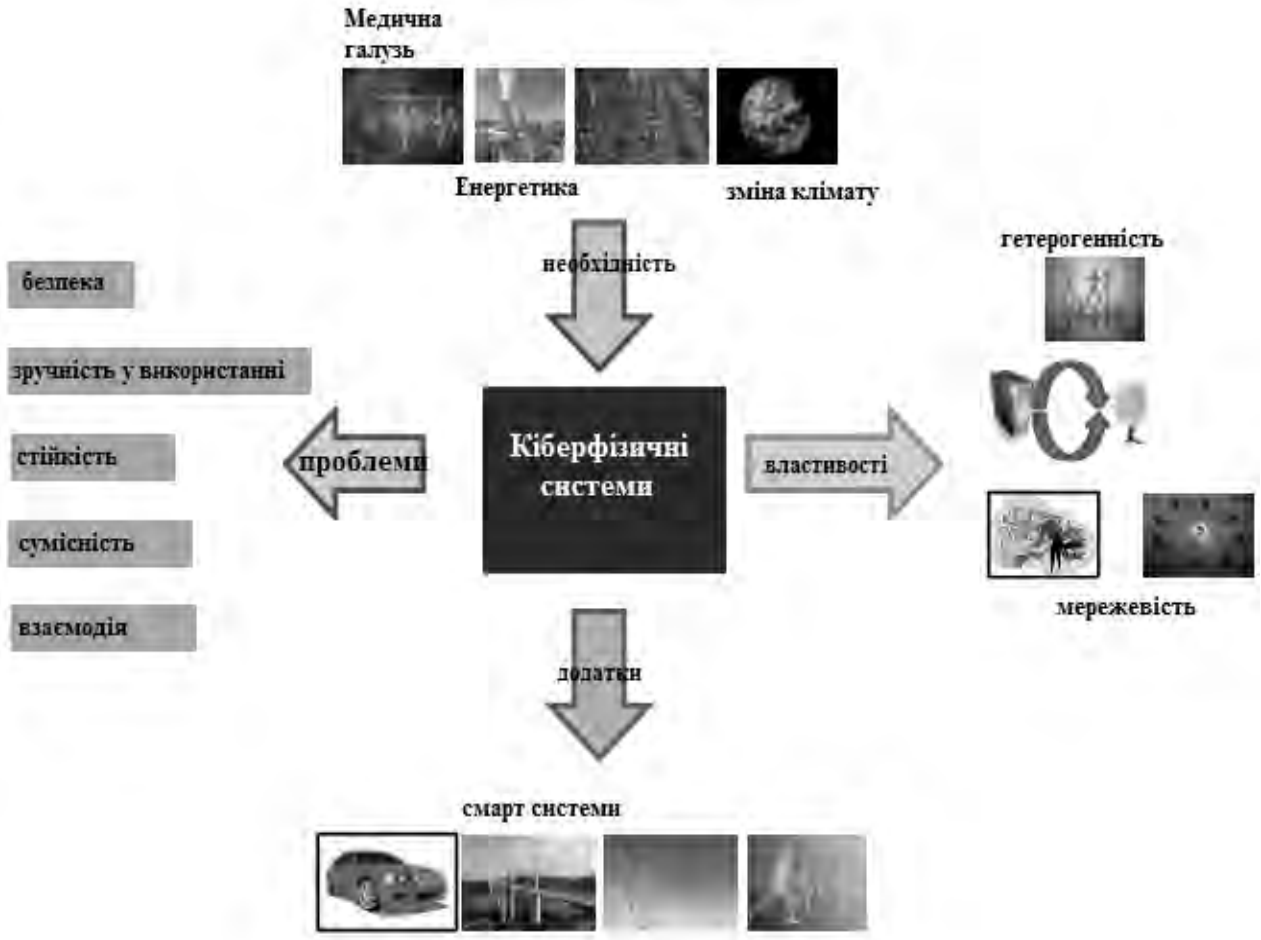

Рис. 1. Кіберфізична система

Незалежно від сфери застосування КФС мають такі основні особливості [2]:

– Залежність від середовища виконання.

КФС дуже тісно пов’язані з середовищем, в якому вони працюють (фізичні об’єкти). Будь-яка зміна в поведінці середовища призводить до зміни поведінки кіберфізичної системи.

– Чітко визначені можливості.

КФС, як правило, складаються з декількох компонентів, які мають різні характеристики. Сенсори, які вбудовані в фізичні пристрої з метою моніторингу, мають обмежені можливості, а програмні засоби, що керують цими сенсорами, є потужнішими.

– Мережевість.

Для КФС, на відміну від традиційних автономних вбудованих систем, потрібен мережевий зв'язок між компонентами для того, щоб вони надали свої послуги.

Принцип роботи КФС

Роботу кіберфізичних систем можна розділити на три етапи [3]:

1. Моніторинг

Це – найголовніший етап у роботі КФС, який полягає в спостереженні за змінами середовища, в якому працює КФС. Він також використовується для отримання відгуків щодо будь-яких дій, які відбувалися у минулому з КФС. Це потрібно для того, щоб уникнути збоїв у системі у майбутньому.

2. Обробка даних

Стосується аналізу даних, зібраних у ході моніторингу для того, щоб дізнатися, чи фізичний процес відповідає попередньо визначеним критеріям. Коли критерії не задовольняються, коригувальні дії визначаються відповідно до інших критеріїв.

3. Виконання

На цьому етапі виконуються дії, визначені на етапі обробки даних. При цьому поведінка КФС може бути змінена повністю.

Будь-яка кіберфізична система може перебувати в одному з трьох можливих режимів: пасивний, пасивно-активний та активний (рис. 2).

Рис. 2. Режими роботи КФС

Пасивний режим – у цьому режимі кіберфізична система не виконує ніяких дій, окрім збирання інформації та контролю середовища (наприклад: медичні прилади).

Пасивно-активний режим – у цьому режимі кіберфізична система контролює своє оточення Якщо певна дія виконується неправильно, тоді відбувається непряме виконання зі зміною поведінки системи. Наприклад: дата-центри виконують smart-планування для того, щоб зменшити температуру в певних місцях.

Активний режим – в цьому режимі кіберфізична система, як і в пасивно-активному режимі, контролює своє середовище. Однак, коли певна дія виконується неправильно, тоді відбувається пряме втручання зі зміною фізичного середовища. Наприклад: системи вентиляції приміщень.

Різновиди атак у КФС

Атака – це будь-яка спроба знищити, вимкнути, вкрасти або отримати несанкціонований доступ до системи [3].

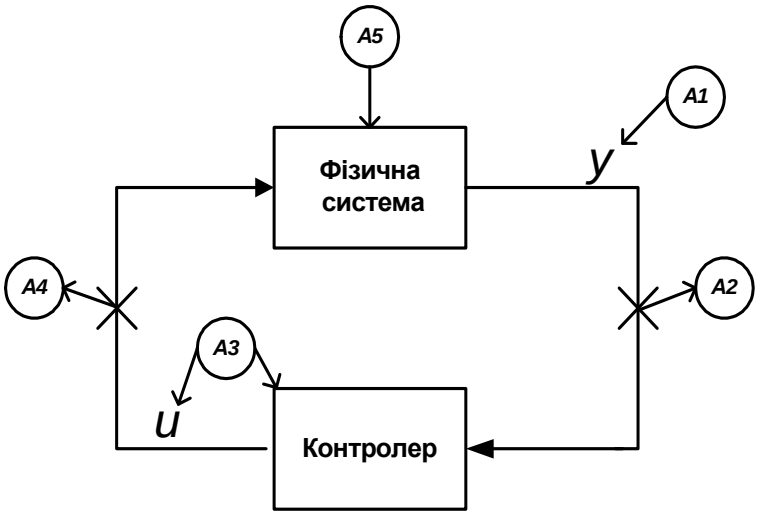

Рис. 3. КФ Атаки

Атаки у КФС (рис. 3) можна класифікувати так [4]:

1. A1 і A2 представляють *обманні атаки,* коли зловмисник із сенсора або контролера відправляє хибне повідомлення. Неправдива інформація може містити неточні виміри, час або інформацію про відправника. У будь-який момент під час атаки система не знає про обман і припускає, що всі дані й послуги, отримані від зловмисника, є законними. Також за такого виду атак зловмисник може перехопити будь-яку інформацію, передану в системі. Такі атаки здійснюються за наявності секретного ключа або за допомогою зламу сенсорів (A1) чи контролерів (A3).

2. A2 і A4 відображають DoS атаки. Зловмисник не дає контролеру отримувати інформацію з фізичної системи. У цьому випадку відбувається проникнення у комунікаційні канали і зловмисник може не тільки отримати доступ до інформації, але й змінити або видалити її. Це також може призвести до некоректного виконання і затримки ініціалізації конкретних послуг.

3. A5 – це прямі атаки на КФС. З алгоритмічної позиції неможливо забезпечити відбиття цих атак (окрім виявлення їх). Тому значні зусилля повинні бути спрямовані на запобігання прямим атакам на фізичні системи.

Хоча A5 атаки і є найбільш руйнівними, вони трапляються нечасто, тому під час розроблення систем захисту інформації необхідно звернути увагу на атаки A1-A4.

Загрози у кіберфізичній безпеці

Для того щоб гарантувати безпеку в кіберфізичних системах, потрібно уникнути багатьох загроз, основними з яких є:

Нечітка модель загроз(Altered Threat Model) – традиційна модель загроз для обчислювальних систем, зосереджена лише на програмних загрозах. Водночас більшість кіберфізичних систем залежні від середовища виконання. Під час атаки зловмисникам не обов'язково спотворювати поведніку фізичної системи, іноді процес зчитування інформації може призвести до виходу з ладу кіберфізичної системи.

Специфічність вимог до безпеки для певних систем (Application Specific Security Requirements) – традиційні вимоги до безпеки можуть бути недостатніми для певних кіберфізичних систем. Тому кожна функція кіберфізичної системи має власний набір заходів безпеки. Наприклад, авторизація у медичній кіберфізичній системі може означати дозвіл отримання певних ліків, тоді як авторизація у кіберфізичній системі типу smart може просто надавати можливість доступу до певних додатків.

Безпечність, орієнтована на користувачів (User-Centric Security), – використання кіберфізичних систем не обмежується спеціалізованими системами. Багато кіберфізичних додатків є системами щоденного використання, користувачі яких, як правило, не обізнані з технікою. Це – системи

медичного моніторингу, смартінфраструктури тощо. Тому рішення безпеки для кіберфізичних систем повинні бути зручними у використанні (plug-n-play функціональності, прозорість безпеки).

Вимоги щодо безпеки у КФС

Для того, щоб уникнути атаки на систему, необхідно дотримуватись таких вимог безпеки.

Конфіденційність

Під конфіденційністю розуміють здатність приховувати дані [5]. Це зазвичай досягається за допомогою криптосистем. Криптосистема – це математична функція, яка перетворює (шифрує) вхідне повідомлення на зашифрований текст. Зашифрований текст може бути перетворений у початковий стан тільки за наявності інверсної функції. Процеси шифрування і розшифрування можуть відбуватися тільки за допомогою криптографічного ключа. Розшифрувати повідомлення практично неможливо, не знаючи точного значення ключа. Існують два типи криптографічних систем, які можна використовувати для забезпечення конфіденційності: симетричні та асиметричні криптосистеми.

Під симетричними криптосистемами розуміють такі криптосистеми, в яких для шифрування і розшифрування використовується той самий ключ [6]. Недоліком цих систем є те, що у разі втрати або викрадення ключа конфіденційність системи втрачається. Деякі з відомих алгоритмів, які використовують симетричний ключ, – AES [7] і RC5 [8].

В асиметричних криптосистемах для шифрування і розшифрування використовуються різні ключі, зв’язані між собою деякою залежністю [9]. При цьому встановити один ключ, знаючи інший, з обчислювального погляду, дуже складно. Один із ключів (наприклад, ключ шифрування) може бути загальнодоступним, і в такому випадку проблема отримання загального секретного ключа не виникає. Відомі такі асиметричні алгоритми: RSA, Діффі–Хеллман.

Цілісність

Щоб забезпечити цілісність даних, потрібно враховувати здатність виявляти будь-які зміни, внесені у передане повідомлення. Це зазвичай роблять за допомогою хеш-функції.

Хеш-функція на вхід приймає дані, цілісність яких потрібно забезпечити, і на вихід подає випадкове значення фіксованої довжини, яке називається збіркою [9]. Оскільки ця функція є односторонньою, то за найменшої зміни вхідних даних результат буде іншим. Для асиметричних сценаріїв хеш-функція використовується для отримання даних, які зашифровані за допомогою приватного ключа – цифрового підпису. Під час перевірки цілісності даних хеш-функція обчислюється за допомогою відкритого ключа, після чого розшифрований текст порівнюється з наявним. Відомі такі алгоритми: MD5 [10], SHA [11].

Аутентифікація

Аутентифікація встановлює рівень довіри між системами, що потім є основою всієї подальшої комунікації. В інтерактивних системах аутентифікація забезпечує розпізнавання системи. Деякими добре відомими методами є цифрові сертифікати, біометричні показники, взаємодії запит–відповідь.

Авторизація

Враховуючи особу суб’єкта, що взаємодіє з системою, авторизація визначає системні дані й керує ними за допомогою моделі керування доступом. В основній формі вона працює так:

1. Особа, яка хоче використовувати об'єкт у системі, робить запит.
2. Модель управління доступом приймає запит й ідентифікує особу, після чого надає їй певні привілеї на основі чітко визначених правил.
3. Якщо запит відповідає привілеям, тоді доступ дозволений.

Криптографічні вимоги у КФС

З наведеного вище можна зробити висновок, що для збереження конфіденційності та захисту цілісності інформації основною вимогою є використання криптографічних методів.

Процес криптографічного закриття даних може здійснюватись як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, проте має і переваги: висока продуктивність, простота, захищеність. Програмна реалізація практичніша і забезпечує більшу гнучкість у використанні.

Незалежно від способу реалізації для сучасних криптографічних систем захисту інформації визначено такі вимоги [6, 12]:

– Знання алгоритму шифрування не повинно знижувати криптостійкість шифру. Цю вимогу сформулював у XIX ст. Керкхофф; криптосистеми поділяються на два види: загального використання (алгоритм доступний потенційному порушнику) і обмеженого використання (алгоритм зберігається в таємниці).

– Вибір криптографічної технології має задовольняти вимоги надійності.

– Зашифроване повідомлення повинно бути прочитаним тільки за наявності ключа.

– Шифр повинен бути стійким, навіть коли зловмиснику відома достатня кількість вхідних даних і відповідних їм зашифрованих даних.

– Незначна зміна ключа або вихідного повідомлення повинна приводити до істотної зміни вигляду зашифрованого тексту.

– Структурні елементи алгоритму шифрування повинні бути незмінними.

– Довжина шифрованого повідомлення повинна дорівнювати довжині вихідного повідомлення.

– Додаткові біти, які вводяться в повідомлення, у процесі шифрування, повинні бути повністю і надійно приховані в шифрованому повідомленні.

– Будь-який ключ із множини можливих повинен забезпечувати рівну криптостійкість.

– Не повинно бути простих і легковстановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування

– Кількість операцій, необхідних для розшифрування інформації з перебором можливих ключів, повинна мати чітку нижню оцінку і або виходити за межі можливостей сучасних комп'ютерів, або потребувати використання дорогих обчислювальних систем.

Висновки

У роботі наведено основні характеристики кіберфізичних систем, а саме: залежність від середовища виконання, чітко визначені можливості та мережевість. Описано такі різновиди атак: обманні атаки, DoS атаки, прямі атаки на КФС. Розглянено властивості безпечності у КФС (конфіденційність, цілісність, аутентифікація, авторизація) та основні загрози у кіберфізичній безпеці (нечітка модель загроз, специфічність вимог до безпеки певних систем, безпечність, орієнтована на користувачів). Сформульовано основні криптографічні вимоги у КФС.

Наукові результати, подані у цій статті, отримано у межах дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015–31.12.2017, фінансово підтриманого Міністерством освіти та науки України.

1. Мельник А. О., Кіберфізичні системи: проблеми створення та напрями розвитку. – Львів: Видавництво Львівської політехніки. – 2014. – С. 154–161. 2. Laura Vegh, Liviu Miclea. Securing Communication in Cyber-Physical Systems using Steganography and Cryptography / Technical University of Cluj-Napoca, Faculty of Automation and Computer Science, Romania, June 2014. 3. Krishna Kumar. Venkatasubramanian, Security solutions for cyber-physical systems, Arizona State University, December 2009. 4. Alvaro A. Cardenas Saurabh Amin, Shankar Sastry, Secure Control: Towards Survivable Cyber-Physical Systems, University of California, Berkeley, August 2013. 5. Saddek Bensalem, Roberto Passerone,Alberto Sangiovanni-Vincentelli,CPS Methods and Techniques,Project co-funded by the European Union's Seventh Framework Programme,July 2013. 6. Elliptic Curve Cryptographic Co-Processor Components for Security On medical Embedded Systems. 7. Daemen J. and Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard. Springer Verlag, 2002. 8. Rivest R. L. The RC5 encryption algorithm. – 1995. – P. 86–96. Workshop on Fast Software Encryption. 9. Баричев С. Г., Серов Р. Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2002. – 175 с. 10. Rivest R. L. The md5 message-digest algorithm (rfc 1321), 1992. 11. Diffie W. and Hellman M. E. New directions in cryptography. ieee transactions on information theory // IEEE Transactions on Information Theory, 22(6):644–654, 1976. 12. Swapna Iyer,Cyber Security for Smart Grid, Cryptography, and Privacy, Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793, USA, July 2011.