Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Проблеми безпеки сучасних кіберфізичних систем

Казакова Н.Ф.
доктор технічних наук, доцент
завідувач кафедри комп'ютерних та інформаційно-вимірювальних технологій
Одеської державної академії технічного регулювання та якості
Щербина Ю.В.
кандидат технічних наук, доцент
доцент кафедри комп'ютерних та інформаційно-вимірювальних технологій
Одеської державної академії технічного регулювання та якості
Фразе-Фразенко О.О.
кандидат технічних наук,
доцент кафедри комп'ютерних та інформаційно-вимірювальних технологій
Одеської державної академії технічного регулювання та якості

Інтеграція сучасних інформаційних технологій створює умови для виникнення як локальних, так і національних кіберфізичних систем. Кіберфізичні системи (Cyber-Physical System, CPS) – це системи, до складу яких входять природні об'єкти та штучні підсистеми, що дозволяють визначати їх як єдине ціле [1]. У CPS зв'язок і координація дій між обчислювальними та фізичними ресурсами забезпечується на новому, більш ефективному, у порівнянні із звичайними автоматизованими системами, рівні. Цикл управління у таких системах передбачає як вплив обчислювальних систем на фізичні процеси, так і навпаки, вплив розвитку фізичних процесів на процедури обчислювання. Таким чином, CPS – це автоматизовані системи, у яких співіснують два типи моделей. З одного боку це традиційні інженерні моделі, а з іншого – комп'ютерні моделі. Це пояснюється тим, що обчислювальні засоби реалізуються як складова фізичних систем і пристроїв.

Сучасні CPS виникли як результат розвитку вбудованих розподілених систем, що функціонують у режимі реального часу. Область їх використання поширюється на такі важливі види людської діяльності, як управління промисловим виробництвом, транспортними системами, енергопостачанням, збройними силами та іншими силовими структурами. Стрімке зростання їх складності та зміна архітектури обчислювальних процесів надає передпосилки для стрімкої зміни парадигми інформаційного захисту. Таким чином, питання інформаційної безпеки CPS потребує значної уваги з боку держави, особливо у аспекті законодавчого регулювання.

Сьогодні найбільший вплив на стратегію технологічного розвитку Європи має Німеччина. У відповідній концепції "Індустрія 4.0" [2] наголошується, що поява кіберфізичних систем стосується не тільки технічних засобів, а й суспільства у цілому. Під час їх створення обов'язково мають братись до уваги соціокультурні аспекти проблеми з урахуванням усіх боків розвитку суспільства. Очікується, що створення повноцінних CPS призведе до на стільки ж значних змін , як і поява всесвітньої комп'ютерної мережі.

У країнах Заходу, у недалекому майбутньому, передбачається поява таких перспективних, як національних, так і наднаціональних кіберфізичних платформ, що включають Інтернет речей, Інтернет людей та Інтернет сервісів. Інтернет речей (Internet of Things and Services) [3] – це технологія, що спрощує життя людей, дозволяючи їм керувати технічними побутовими засобами через доступні інтерфейси, наприклад, за допомогою комп'ютерів, смартфонів тощо. Під Інтернетом людей (Internet of People, IoP) [4] розуміється технологія майбутнього, яка дозволить адаптувати навколишнє середовище до вимог комфортного життя конкретної людини без її особистої участі. Якщо перша технологія вже реалізується у багатьох розвинених регіонах світу, то друга – існує лише як сукупність намірів і до кінця не сформульована. Що ж стосується Інтернету сервісів, то сьогодні це, насамперед, доступ до інформаційних ресурсів, мережна торгівля, освіта тощо. Коло сервісних послуг у глобальній мережі постійно удосконалюється та розширюється.

Можливість практичного створення реальних кіберфізичних систем обґрунтовується, по-перше, зростанням числа пристроїв із вбудованими мікропроцесорами і засобами зберігання даних, по друге, інтеграцією Інтернету, технічних систем і послуг, що вони надають у одну загальну складну організаційно-технічну систему, яка утворює "розумне середовище існування" для людей (Smart Building Environment). Вже сьогодні існують надвеликі системи автоматизованого технологічного управління енергопостачанням цілих континентів, наприклад, північноамериканського континенту, залізничними комунікаціями, авіалініями тощо.

Сьогодні панує спрощене розуміння терміну "кіберфізичні системи". Кіберфізична система – це не просто система, що передбачає інтеграцію обчислювальних засобів у фізичні процеси, а система, яка

передбачає впровадження в процеси управління елементів штучного інтелекту. Це необхідно через те, що людина вже не здатна забезпечувати ефективне управління у рамках існуючих автоматизованих систем надзвичайно складними виробничими, технологічними і соціальними процесами. Тобто термін "кібернетичний" не є синонімом слова "мережний". Поки що не вдалось створити обчислювальні системи, які б могли мислити як людина і використовувати усі переваги, що має техніка. Як завжди буває, просування у сторону вирішення складної проблеми відбувається поступово і малими кроками. Але вже сьогодні є достатньо складні системи, що забезпечують управління надзвичайно складними процесами і використовують при цьому такі сучасні складні інформаційні технології як бази і банки даних, системи підтримки прийняття рішень, бази знань і експертні системи.

Разом з тим, розширення можливостей обчислювальних систем і комунікацій призводить до збільшення можливостей скоєння злочинів в кібернетичній сфері. Такі терміни, як Cyberbullying (шкільне мережне насилля), Cybercrime (Мережна злочинність), Cyberterrorism (Мережний тероризм), Cyberwarfare (Мережна війна) тощо, вже міцно ввійшли в сучасне життя. Усі ці поняття жодним чином не пов'язані із кібернетикою, і виникли задовго до появи CPS. Їх існування свідчить про те, що людство і кожна держава окремо, повинні бути готові до боротьби із негативними наслідками технічного прогресу. Зрозуміло, що поява систем розподіленого управління побудованого на нових науково-технічних принципах, поставить і нові задачі з забезпечення захисту процесів, стороннє втручання у які, у більшості випадків, може мати дуже значні наслідки.

На першому плані, як і раніше стоїть проблема несанкціонованого доступу до інформації з обмеженим доступом. Мають бути вирішеними проблеми, пов'язані з регулюванням державою сфери міжмашинної взаємодії у кіберфізичному просторі. На основі наукового аналізу і накопиченого світового досвіду повинні бути розроблені та прийняті відповідні національні стандарти, а також визначена відповідальність за будь-які несанкціоновані дії щодо інформаційних процесів під час обробки великих масивів даних.

Ці задачі можуть бути вирішені лише широким колом фахівців у сфері захисту на основі наукового системного підходу. Має бути визначений порядок інформаційної трансграничної взаємодії, умови зберігання великих даних на серверах, розташованих на території держави, а також створені механізми контролю використання масивів великих даних [5].

Створення систем інформаційної безпеки, що будуть здатні забезпечити захист від загроз нового типу, потребує нової методики і системи аналізу та оцінки загроз, а також відповідних показників безпеки. Для машинних і когнітивних інтерфейсів, повинен бути створений новий правовий режим функціонування, який визначить правила реагування на конфліктні ситуації між суб'єктами міжмашинної взаємодії.

Сьогодні кіберфізичні системи – це, здебільшого, теоретичне передбачення. Справді існують надвеликі автоматизовані системи управління, фізичною основою яких є надзвичайно розподілені і надзвичайно складні обчислювальні системи. Але сьогодні вони залишаються лише автоматизованими системами. Не зважаючи на існування достатньо ефективних баз і банків даних, системи підтримки прийняття рішень і експертні системи, створені для вирішення широкого кола задач у різноманітних галузях людської діяльності, якісного прориву у справі створення штучного інтелекту не зроблено, і людина поки що залишається головною складовою системи управління. Проте, втілення обчислювальних систем, побудованих на основі сучасних мікропроцесорів та мікроконтролерів, до складу виконавчих механізмів суттєво змінює архітектуру автоматизованих систем управління, яка існувала протягом кількох останніх десятиріч. Це в свою чергу викликає необхідність розроблення нових, визначених на нормативному рівні, правил їх використання.

Література:

1. Леонид Черняк. Интернет вещей: новые вызовы и новые технологии // Открытые системы. СУБД. — 2013. — № 4. — С. 14–18. URL: http://www.osp.ru/os/2013/04/13035551 (дата обращения: 11.03.2014).

2. Colombo A., Bangemann T. Industrial Cloud-based Cyber-physical Systems: The IMC-AESOP Approach. Cham Springer International Publishing, 2014. – 245 p.

3. L. Atzori, A. Iera, G. Morabito. From «Smart Objects» to «Social Objects»: The Next Evolutionary Step of the Internet of Things // IEEE Comm. — 2014. Vol. 52, № 1. — P. 97–105.

4. J. Gubbi et al. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions // Future Generation Computer Systems. — 2013. Vol. 29, № 7. — P. 1645–1660.

5. N. Makitalo et al. Social Devices: Collaborative Co-located Interactions in a Mobile Cloud // Proc. 11th Int'l Conf. Mobile and Ubiquitous Multimedia. — 2012. Article № 10.