УДК 004.056

В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець

Національний університет "Львівська політехніка", Львів

КОМУНІКАЦІЙНЕ СЕРЕДОВИЩЕ КІБЕРФІЗИЧНОЇ СИСТЕМИ "WI-FI – BLUETOOTH – ХМАРНІ ОБЧИСЛЕННЯ – IOT": ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Проаналізовано інформаційну безпеку (ІБ) комунікаційного середовища (КС) кіберфізичної системи (КФС): Wi-Fi, Bluetooth, хмарні обчислення, IoT. Розглянуто особливості найпоширеніших моделей управління ІБ у контексті їх застосування до зазначених технологій зв'язку.

Ключові слова: *кіберфізична система, комунікаційне середовище, Wi-Fi, Bluetooth, хмарні обчислення, IoT, інформаційна безпека, модель управління.*

Вступ

Актуальність. В сучасних умовах інформатизації та інтелектуалізації суспільства актуальними є питання створення та застосування кіберфізичних систем. В контексті безпечного функціонування таких систем існує проблема забезпечення ІБ складових КФС, зокрема КС, структуру якого формують, зокрема: Wi-Fi, Bluetooth, хмарні обчислення, IoT. Функціональна та інформаційна безпека КФС є підґрунтям ефективної реалізації задач контролю, обробки та керування. Модифікація КФС відповідно до функціональних задач вимагає вдосконалення методів і засобів ІБ, а також моделей управління ІБ, зокрема у частині безпровідних технологій зв'язку. Відповідно до Проекту Концепції інформаційної безпеки України існує потреба у захищеності кібернетичних, телекомунікаційних та інших комп'ютеризованих систем, що формують інфраструктуру інформаційного простору [1].

Постановка задачі і мета роботи. Технічний прогрес суспільства у напрямі інтеграції в глобальний інформаційний простір передбачає широке застосування кіберфізичних систем в різних інфраструктурах суспільства. З метою забезпечення ІБ таких систем актуальним є міжнародне науково-технічне співробітництво України в межах Рамкової програми "Горизонт – 2020", зокрема у сегменті розвитку нового покоління комп'ютеризованих систем. Для забезпечення конфіденційності, цілісності та доступності інформації в комунікаційному середовищі КФС необхідно проаналізувати аспекти ІБ сучасних технологій зв'язку Wi-Fi, Bluetooth, хмарних обчислень та IoT. Мета роботи – провести аналіз та синтез елементів захисту інформації в КС кіберфізичної системи і розглянути моделі управління інформаційною безпекою.

Інформаційна безпека КС "Wi-Fi – Bluetooth – хмарні обчислення – IoT"

Проаналізуємо інформаційну безпеку КС відповідно на рівні Wi-Fi, Bluetooth, хмарні обчислення, IoT адекватно до системи загроз згідно зі структурою концепції багаторівневої комплексної системи безпеки КФС [2].

Аспекти захисту Wi-Fi. Технологія безпровідного зв'язку Wi-Fi ґрунтується на сімействі стандартів IEEE 802.11 і забезпечує гарантовану сумісність будь-якого обладнання та можливість створення захищеної мережі з використанням надійного шифрування. Концепція "об'єкт – загроза – захист" для Wi-Fi сформована на рівнях моделі OSI. Приклади загроз для Wi-Fi на рівнях OSI: прикладному – несанкціоноване одержання прав на доступ; представлення – припинення виконання необхідних функцій; сеансовому – несанкціоноване завершення, переадресація сеансу; транспортному – несанкціонована підміна пакетів; мережевому – читання, модифікація, знищення даних; фізичному – відмови в обслуговуванні; канальному – атаки на пароль доступу. Захист Wi-Fi на рівні: прикладному – ідентифікація та аутентифікація користувачів; представлення – фільтрація потоку пакетів; сеансовому – перевірка автентичності клієнта та сервера; транспортному – шифрування даних; мережевому – протокол IPSEC; фізичному – MAC-фільтрацію; канальному – аутентифікація користувачів.

Безпека Bluetooth. Технологія економічного бездротового зв'язку на малих відстанях Bluetooth передбачає підтримку швидкого підключення, можливість використання пристроїв малої потужності та сумісність обладнання різних поколінь. Для Bluetooth, яка функціонує на фізичному рівні OSI, характерні такі загрози / захист відповідно до протоколів: LMP (Link Management Protocol) – підміна пристроїв / ідентифікація, аутентифікація пристроїв; HCI (Host/controller interface) – відправка помилкових статусів підключення / шифрування статусів; AVRCP (A/V Remote Control Profile) – перехоплення голосових повідомлень / шифрування повідомлень; L2CAP (Logical Link Control and Adaptation Protocol) – помилки мультиплексувань з'єднань / ведення журналів помилок; SDP (Service Discovery Protocol) – несанкціоноване використання послуг / ідентифікація, аутентифікація користувачів; RFCOMM (Radio Frequency Communications) –

© В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець

збої емуляції / застосування преемуляції; BNEP (Bluetooth Network Encapsulation Protocol) – перехоплення даних / шифрування даних; AVCTP (Audio/Video Control Transport Protocol) – несанкціонована зміна команд / ускладнення синтаксису команд; AVDTP (Audio/Video Distribution Transport Protocol) – переривання зв'язку / зменшення затримки повторного підключення; TCS (Telephony Control Protocol) – переадресація викликів / авторизація пристроїв та користувачів.

Захист інформації в хмарних обчисленнях. Хмарні обчислення (cloud computing) – це модель забезпечення повсюдного і зручного мережевого доступу на вимогу до загального набору конфігурованих обчислювальних ресурсів, зокрема в контексті КФС до технологій передавання даних. В залежності від моделі розгортання застосовуються такі структури хмарних технологій: private cloud (використання однією організацією); public cloud (вільне використання різними організаціями); hybrid cloud (комбінація двох або більше хмарних інфраструктур з різними правами доступу та стандартизованими технологіями передавання даних і додатків); community cloud (використання конкретною спільнотою споживачів з організації). З позиції ІБ для хмарних обчислень характерні такі апаратні загрози: несанкціонований фізичний доступ до обладнання та серверів хмари; відмови, збої, аварії обладнання; помилки при конфігуруванні. Приклад програмних загроз: несанкціонований віддалений доступ до ресурсів хмари; шкідливе програмне забезпечення; експлойти. Апаратний захист хмарних технологій передбачає: обмеження доступу до обладнання та серверів; використання сертифікованого обладнання; ведення журналу дій користувачів. На програмному рівні захисту застосовуються: ідентифікація, аутентифікація користувачів хмарних ресурсів; шифрування даних; своєчасне оновлення програмного та антивірусного забезпечення. Для шифрування даних в хмарних обчисленнях доцільно використовувати спеціалізовані криптографічні системи (табл. 1).

Таблиця 1

Характеристика криптографічних систем для шифрування даних в хмарних обчисленнях

Назва системи	Алгоритми роботи	Особливості	Нормативне забезпечення
Luna CA4	RSA, RC2, RC4, RC5, CAST-3, CAST-128, AES. ARIA, SHA-1. MD-2, MD-5, SHA256, SHA512, SHA-224, SHA-384, HMAC- MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC	• надійне зберігання кореневих ключів сертифікатних центрів в інфраструктурах відкритих ключів (PKI); • гнучке збільшення продуктивності; • підтримка основних сертифікатів	PKCS 9 1 vl.5, 0AEPPKCS31 v2.0, FIPS 140- 2
Luna PCI	RSA. DSA. DES. 3DES.AES, RC2, RC4, RCS, CAST-3, CAST- 128. HMAC-MD5, HMAC-SHA- 1, SSL3-MD5-MAC, SSL3-SHA- 1-MAC, SHA-1. MD-2. MD-5, SHA256, SHA512	• дуже висока продуктивність (до 7000 операцій RSA-1024 Sign в секунду); • гарантований захист і контроль ключів з моменту генерації до утилізації	PKCS 9 1 vl.5, OAEP PKCS # 1 v2.0, FIPS 140- 2
ProtectServer Gold	RSA (до 4096 біт). DSA, EC- DSA, Diffie Heilman (DH). AES. DES, 3DES, CAST-128, RC2. RC4, SEED. ARIA, SHA-1, SHA- 256. SHA-384. SHA-512.MD2, RIPEMD128, IPEMD160. DES MDC-2 PAD1, SSL3 MD5 MAC, DES3 MAC. DES3 Retail CEB MAC.	• високий рівень захисту для PKI; • широкий набір програмних інтерфейсів; • наявність 4 Мб захищеної пам'яті для зберігання ключів і програмного коду.	PKCS 9 1 vl.5. OAEP PKCS 91 v2.0, FIPS 140- 2, FCC Part 15
nShield Solo	AES, Aria, Camelia, Triple DES, RSA, Diffie-Heilman, DSA, ECC Suite B. SHA-1, SHA-2.	• застосування інтерфейсу PCI; • можливість включення в апаратний модуль системи безпеки (HSM); • відповідність найвищим вимогам до продуктивності та безпеки	FIPS 140-2, EAL 4+
TrueCrypt	AES (256). Blow- fish (448), CASTS (128). Serpent (256). Triple DES, Twofish (256).	• можливість програмної зміни довжини ключа (128-448 біт); • можливість створення зашифрованого віртуального диска	Open Source

Безпека Інтернету речей (Internet of Things (IoT)). IoT – технологія зв'язку, що зв'язує пристрої, які мають автономне забезпечення, керуються інтелектуальними системами, забезпечені високорівневою операційною системою, автономно підключені до Інтернету і можуть виконувати власні чи хмарні обчислення та аналізувати зібрані дані. IoT у структурі КФС забезпечує зв'язок високотехнологічних пристроїв обробки та зберігання інформації з інтелектуальними системами (давачами) за допомогою технологій КС (Wi-Fi, Bluetooth, хмарні обчислення). Для IoT характерними є такі апаратні загрози: помилки при конфігуруванні обладнання; несанкціонована зміна параметрів обладнання; збої, відмови, аварії апаратури; підміна пристроїв; несанкціоноване віддалене керування. Програмними загрозами є: застосування помилкових параметрів програмного забезпечення; атаки DoS / DDoS; фішинг; програмні збої; атаки на паролі; бот-мережі. Апаратний захист IoT включає: ведення журналу подій; обмеження доступу до обладнання; апаратне шифрування інформації; фільтрацію пакетів, адрес; резервне копіювання; ідентифікацію апаратури. Для програмного захисту застосовується: своєчасне оновлення програм; механізми ідентифікації та аутентифікації користувачів; сертифіковані програми; антивірусне програмне забезпечення.

Моделі управління ІБ комунікаційного середовища

Розглянемо особливості найпоширеніших моделей управління ІБ DMAIC, SWOT, 8D та PDCA.

DMAIC (“визначення – вимірювання – аналіз – вдосконалення – контроль”) функціонує на основі застосування проектного підходу і статистичних методів. В основі моделі знаходяться три взаємозалежні елементи: покращення існуючих процесів; проектування нових процесів; управління процесами. Етапи застосування DMAIC: Define – визначення цілей проекту і запитів користувачів; Measure – вимірювання процесу для визначення стану поточного виконання; Analyse – аналіз та визначення глибинних причин дефектів; Improve – покращення процесу через скорочення дефектів; Control – контроль подальшого протікання процесу.

SWOT (“сильні сторони – слабкі сторони – можливості – загрози”) передбачає аналіз сильних і слабких сторін об’єкта (внутрішнє середовище), а також можливостей та загроз (зовнішнє середовище). Етапи моделі: збір інформації; зіставлення сильних та слабких сторін об’єкта та факторів зовнішнього середовища, побудова матриці взаємозв’язків; вироблення стратегічних рішень для кожного варіанту матриці.

Модель управління ІБ 8D включає вісім послідовних кроків для вирішення певної проблеми з документуванням результатів для накопичення досвіду. Кроки моделі 8D: створення міжфункціональної команди фахівців; опис проблеми; розробка тимчасових заходів; визначення та перевірка першопричини; розробка коригувальних дій; попередження повторення проблеми; підведення підсумків та збереження досвіду.

Модель *PDCA* (“плануй – виконуй – перевіряй – дій”) застосовується до процесів системи управління інформаційною безпекою (СУІБ) – розробка, впровадження та забезпечення функціонування, підтримка та вдосконалення, моніторинг та перегляд. PDCA функціонує на основі таких етапів: плануй – розробка політики ІБ, суттєвих цілей, процесів та процедур; виконуй – впровадження та забезпечення функціонування політики ІБ, контролів, процесів та процедур СУІБ; перевіряй – оцінювання та вимірювання продуктивності процесів згідно з політикою, цілями і практичним досвідом СУІБ; дій – застосування коригувальних та запобіжних заходів на підставі результатів внутрішнього аудиту і перегляду СУІБ. Приклад застосування моделі PDCA до безпровідних технологій зв’язку комунікаційного середовища КФС: плануй – сформована політика ІБ передбачає використання механізмів ідентифікації та аутентифікації користувачів; виконуй – забезпечення функціонування зазначених механізмів зі стандартними параметрами для кожної з технологій; перевіряй – виявлення вразливості механізмів, що дозволяє обійти захист; дій – зміна параметрів та конфігурації механізмів ідентифікації та аутентифікації, що значно ускладнюють обхід захисту (збільшення довжини, складності логіна / пароля, використання біометричних методів, одноразової ідентифікації, аутентифікації).

Висновки

Розглянуто елементи ІБ комунікаційного середовища КФС, зокрема аспекти захисту Wi-Fi на основі моделі OSI; загрози та захист Bluetooth відповідно до протоколів функціонування; безпеку хмарних обчислень із застосуванням криптографічних систем; апаратний та програмний захист IoT відповідно до загроз. Проаналізовано найпоширеніші моделі управління ІБ у контексті їх застосування до КС кіберфізичної системи.

Список літератури

1. Проект Концепції інформаційної безпеки України. – [Електронний ресурс]. – Режим доступу до ресурсу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

2. Дудикевич В.Б. Парадигма та концепція побудови багаторівневої комплексної системи безпеки кіберфізичних систем / В.Б. Дудикевич, В.М. Максимович, Г.В. Микитин // Вісник Національного університету “Львівська політехніка”. Автоматика, вимірювання та керування. – 2015. – № 821. – С 3-7.

Надійшла до редколегії 1.03.2016

Рецензент: д-р техн. наук, проф. Л.Т. Пархуць, Національний університет «Львівська політехніка», Львів.

КОММУНИКАЦИОННАЯ СРЕДА КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ “WI-FI – BLUETOOTH – ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ – IOT”: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В.Б. Дудыкевич, Г.В. Микитин, А.И. Ребец

Проанализирована информационная безопасность (ИБ) коммуникационной среды (КС) киберфизической системы (КФС): Wi-Fi, Bluetooth, облачные вычисления, IoT. Рассмотрены особенности наиболее распространенных моделей управления ИБ в контексте их применения в указанных технологиях связи.

Ключевые слова: *киберфизическая система, коммуникационная среда, Wi-Fi, Bluetooth, облачные вычисления, IoT, информационная безопасность, модель управления.*

THE COMMUNICATION ENVIRONMENT OF A CYBER-PHYSICAL SYSTEM “WI-FI – BLUETOOTH – CLOUD COMPUTING – IOT”: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT MODELS

V.B. Dudykevych, G.V. Mykytyn, A.I. Rebets

An information security (IS) of the cyber-physical system (CPS) communication environment (CE): Wi-Fi, Bluetooth, cloud computing, IoT was analyzed. Main IS management models features were reviewed in the context of their use of these communication technologies.

Keywords: *cyber-physical system, communication environment, Wi-Fi, Bluetooth, cloud computing, IoT, information security, management model.*