УДК 004.056 DOI: 10.30748/soi.2017.148.16

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

Національний університет "Львівська політехніка", Львів

КОМПЛЕКСНА СИСТЕМА БЕЗПЕКИ КІБЕРФІЗИЧНОЇ СИСТЕМИ "IPHONE – WI-FI, BLUETOOTH – ДАВАЧІ"

Запропоновано підхід до створення комплексної системи безпеки (КСБ) кіберфізичної системи (КФС) "iPhone – Wi-Fi, Bluetooth – давачі" відповідно до стандарту ISO/ IEC 15408 за впливу загроз, класифікованих за методикою STRIDE. Розроблено системну модель КСБ кіберфізичної системи на рівнях кібернетичного простору (КП), комунікаційного середовища (КС) та фізичного простору (ФП) для забезпечення задач безпеки – конфіденційності (К), цілісності (Ц), доступності (Д), спостережуваності (С) та гарантованості (Г) згідно із запропонованим підходом. Проаналізовано технології захисту інформації у КФС від загроз STRIDE відповідно до задач безпеки.

Ключові слова: *кіберфізична система, комплексна система безпеки, підхід, системна модель, загрози, профілі безпеки, технології захисту інформації.*

Вступ

Процеси інтелектуалізації суспільства актуалізують проблему створення, застосування та забезпечення безпеки кіберфізичних систем у різних предметних сферах.

Безпека кібернетичного простору, комунікаційних систем та об'єктів фізичного простору є одним з пріоритетних векторів державної політики у сфері кібербезпеки [1]. Стратегія кібербезпеки орієнтована на створення нових підходів до забезпечення інформаційної безпеки КФС [2]. Функціональна багаторівневість КФС змінюється відповідно до КП, КС та ФП. Наприклад, для моніторингу стану об'єктів промислової та інтелектуальної інфраструктури ефективною є КФС: смартфон iPhone – технології безпровідного зв'язку Wi-Fi, Bluetooth – МЕМС-давачі.

Постановка задачі. З метою забезпечення конфіденційності, цілісності, доступності, спостережуваності, гарантованості інформації в КФС необхідно розробити підхід до створення КСБ відповідно до вимог стандарту ISO/ IEC 15408 і, на цій основі, створити системну модель КСБ, які є методологічним підгрунтям створення інструментарію інформаційної безпеки (ІБ).

Основний матеріал

1. Підхід до створення комплексної системи безпеки КФС. Структура підходу до створення КСБ представлена у просторі "загрози: STRIDE – профілі: К, Ц, Д, С, Г – інструментарій: механізми, технології безпеки" (рис. 1). Вихідним етапом у створення КСБ є обгрунтування вибору профілів безпеки КФС. Конфіденційність полягає у неможливості доступу до інформації неавторизованим користувачам. Цілісність – неавторизований користувач або процес не може здійснювати модифікацію даних. Доступність – можливість використання ресурсу авторизованим користувачем з виконанням правил політики безпеки. Спостережуваність – можливість реєстрації будь-якої діяльності користувачів чи процесів та ідентифікувати їх. Гарантованість – забезпечення певного рівня впевненості у формуванні та реалізації певних функціональних вимог та заходів захисту [3].

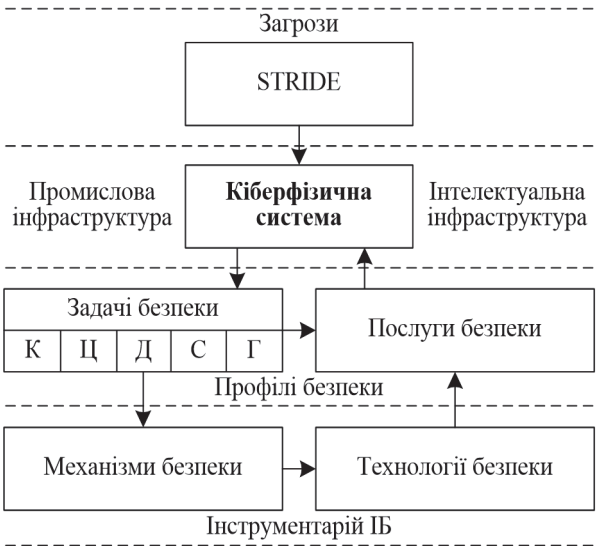

Рис. 1. Підхід до створення комплексної системи безпеки КФС у просторі "загрози – профілі – інструментарій"

З метою забезпечення вибраних профілів безпеки КФС формуються відповідні послуги безпеки – опорні; запобігання; виявлення порушень і відновлення безпеки. Інструментарієм створення КСБ є механізми (загальні, спеціальні) і технології (методи

і засоби) безпеки, які розробляються відповідно до послуг і задач безпеки та забезпечують захист інформації на кожному рівні КФС та відповідно захищений міжрівневий обмін.

2. Системна модель КСБ кіберфізичної системи. Системна модель комплексної системи безпеки кіберфізичної системи “iPhone – Wi-Fi, Bluetooth – давачі” представлена на рис. 2.

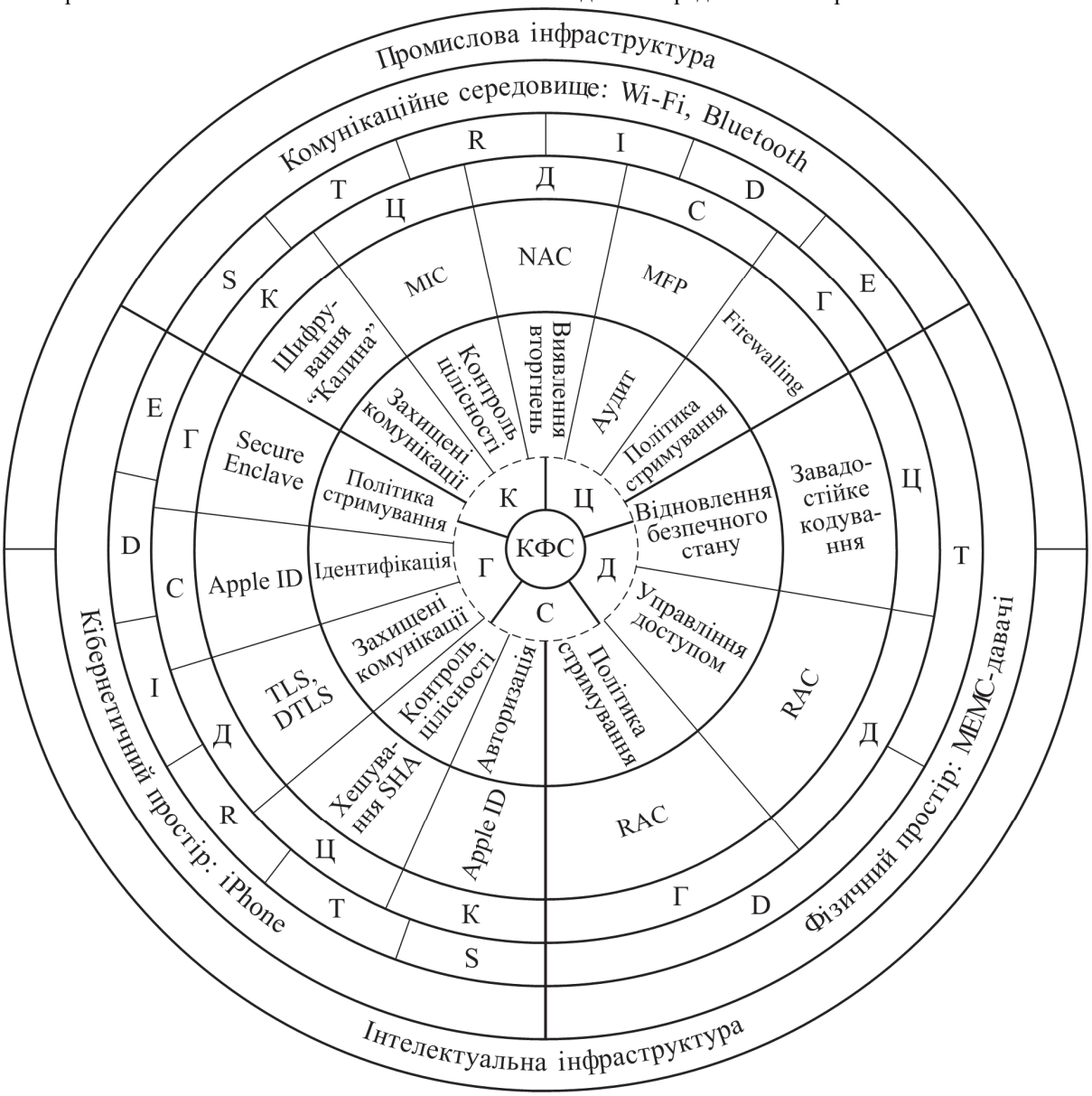

Рис. 2. Системна модель комплексної системи безпеки кіберфізичної системи

Системна модель КСБ кіберфізичної системи складається з підсистем – комплексних систем безпеки КП, КС та ФП, що орієнтовані на забезпечення задач безпеки процесів відбору, обробки, збереження, передавання даних. Зокрема, для КП та КС, представлених смартфоном iPhone та технологіями безпровідного зв’язку Wi-Fi, Bluetooth характерні профілі безпеки – К, Ц, Д, С, Г, а для ФП, який формують МЕМС-давачі, – Ц, Д, Г. На сегменти КФС впливають відповідні загрози, класифіковані за методикою STRIDE: КП, КС – підміна об’єктів (S), модифікація даних (T), відмова від авторства (R), розголошення інформації (I), відмова в обслуговуванні (D), підвищення привілеїв (E); ФП – T, D. Відповідно до цієї класифікації найбільш характерними загрозами для КФС є: S – соціальна інженерія, атаки man-in-the-middle, підміна основного сервера, підміна користувачів; T – несанкціонована зміна кодів доступу, знищення інформації з носіїв, модифікація даних під час передавання по мережі, ненадійність системи резервного копіювання; R – видалення даних про здійснені дії, несанкціоноване використання реєстраційних даних, відсутність / недосконаліть механізму реєстрації подій, маскування несанкціонований дій під помилки; I – перехоплення даних під час передавання через мережу, викрадення носіїв інформації, витік інформації через недостатню кваліфікацію, несанкціонований доступ до

облікових даних; D – DoS / DDoS-атаки флудинг, виведення з ладу вузлів КФС, програмно-апаратні збої / відмови; E – заміна цифрових сертифікатів / підписів, несанкціоноване редагування облікових даних, зміна прав доступу за допомогою шкідливого програмного забезпечення, несанкціонований доступ до службової адміністративної інформації.

Комплексна система безпеки багаторівневої КФС структурована у просторі "рівень КФС – загроза STRIDE – профіль безпеки – технологія захисту інформації". Відповідно структура КСБ кібернетичного простору КФС – смартфона iPhone: К – авторизація – Apple ID; Ц – контроль цілісності – хешування SHA; Д – захищені комунікації – TLS, DTLS; С – ідентифікація – Apple ID; Г – політика стримування – Secure Enclave. Структура КСБ комунікаційного середовища КФС – технологій безпровідного зв'язку Wi-Fi, Bluetooth: К – захищені комунікації – шифрування: "Калина"; Ц – контроль цілісності – MIC; Д – виявлення вторгнень – NAC; С – аудит – MFP; Г – політика стримування – Firewalling. Структура КСБ фізичного простору КФС, який включає MEMC-давачі: Ц – відновлення безпечного стану – завадостійке кодування; Д – управління доступом – RAC; Г – політика стримування – RAC.

У табл. 1. наведена функціональна структура КСБ КФС "загрози – профілі – технології захисту" згідно підходу та системної моделі.

Таблиця 1

Комплексна система безпеки КФС у просторі "загрози – профілі – технології"

Задача безпеки	**Технології захисту інформації у КФС**		
	КП / STRIDE	**КС / STRIDE**	**ФП / TD**
Конфіденційність	• SSL, VPN / несанкціонований віддалений доступ (I); • ARM's Execute Never / несанкціоноване виконання програмного забезпечення (I); • періодичне оновлення операційної системи та програм / використання вразливостей операційної системи (E)	• IPSEC / перехоплення пакетів (I); • VPN / несанкціонований збір інформації про мережу (I); • шифрування кодів доступу / перехоплення кодів доступу (S)	–
Цілісність	• захисне кодування / модифікація кодів доступу (T); • низькорівневе шифрування AES-256 / одержання повного доступу до файлової системи (Jailbreak) (T); • сертифікація операційної системи / несанкціонований запуск функції знищення даних (T)	• IPSEC / маніпуляція біта-ми (атаки bit-flipping) (T); • моніторинг підключень до мережі / виведення з ладу сеансових шлюзів (T); • хешування / виникнення помилок в потоці даних (T)	• механізм здійснення контрольних вимірювань / модифікація показів (T)
Доступність	• ланцюг довіреного завантаження пристрою / експлойти на рівні завантажувача системного ядра (D); • сертифікація Apple Root / експлойти на рівні ядра системи (D); • Apple Sandbox / несанкціонований запуск функції блокування пристрою (D)	• фільтрування пакетів / атаки DoS, DDoS (D); • обмеження доступу до елементів мережі / виведення з ладу елементів мережі (D); • періодичне тестування мережі / помилки мережі (D)	• дублювання давача / перебої електроживлення (D); • аварійне вимкнення давача / перевищення порогових значень (D); • самодіагностика / апаратні відмови (D)
Спостережуваність	• технологія фіксації дій користувача / заміна цифрових сертифікатів, підписів (R); • сертифікація програм / маскування шкідливого програмного забезпечення (R); • дактилоскопічний давач /	• віддалене збереження log-файлів / маскування несанкціонованих налаштувань (R); • ідентифікація, аутентифікація користувачів / несанкціоноване використання ресурсів	–

Закінчення табл. 1.

Задача безпеки	Технології захисту інформації у КФС		
	КП / STRIDE	**КС / STRIDE**	**ФП / TD**
Спостережуваність	несанкціоновані покупки через програми (R)	мережі (R); • обмеження доступу до облікових даних та послуг / несанкціоноване використання/ зміна послуг (R)	
Гарантованість	• сертифікація програм та пристроїв / соціальна інженерія (S); • сертифікація прошивки SHSH / підміна об'єктів (S); • періодичне оновлення операційної системи та програм / використання вразливостей операційної системи (E)	• ідентифікація обладнання / під-міна пристроїв (атака man-in-the-middle) (S); • багатофакторне підтвердження змін / несанкціонована зміна статусів підключення (E); • ідентифікація учасників сеансу / несанкціонована зміна прав доступу (E);	• механізм здійснення контрольних вимірювань / модифікація показів (T); • самодіагностика / апаратні відмови (D)

Висновок

Запропоновано підхід до створення КСБ КФС згідно ISO/ IEC 15408 та системну модель у просторі "загрози – профілі – інструментарій", що дає підстави для забезпечення захищеного відбору даних, захищеної обробки, зберігання та передавання інформації, відповідно безпечного функціонування КФС та її компонентів.

Список літератури

1. Проект Закону України "Про основні засади забезпечення кібербезпеки України" від 19.06.2015 № 2126а. – [Електронний ресурс]. – Режим доступу: http:// w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

2. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"" від 15.03.2016 № 96/2016. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016.

3. Information technology. Security techniques. Evaluation criteria for IT security. Parts 1, 2, 3: ISO/IEC 15408-1, 2, 3. – [Approved 2008-2009]. – Switzerland: ISO copyright office, 2008-2009. – 456 p.

Надійшла до редколегії 25.02.2017

Рецензент: д-р физ-мат. наук проф. С.Е. Остапов, Черновицкий национальный университет имени Юрия Федьковича, Черновцы.

КОМПЛЕКСНАЯ СИСТЕМА БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ "IPHONE – WI-FI, BLUETOOTH – ДАТЧИКИ"

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

Предложен подход к созданию комплексной системы безопасности (КСБ) киберфизической системы (КФС) "iPhone – Wi-Fi, Bluetooth – датчики" в соответствии со стандартом ISO / IEC 15408 при воздействии угроз, классифицированных по методике STRIDE. Разработана системная модель КСБ киберфизической системы на уровнях кибернетического пространства (КП), коммуникационной среды (КС) и физического пространства (ФП) для обеспечения задач безопасности – конфиденциальности (К), целостности (Ц), доступности (Д), наблюдаемости (С) и гарантированности (Г) согласно предложенному подходу. Проанализированы технологии защиты информации в КФС от угроз STRIDE в соответствии с задачами безопасности.

Ключевые слова: *киберфизическая система, комплексная система безопасности, подход, системная модель, угрозы, профили безопасности, технологии защиты информации.*

THE COMPLEX SECURITY SYSTEM OF THE CYBER-PHYSICAL SYSTEM "IPHONE – WI-FI, BLUETOOTH - SENSORS"

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

The approach to the complex security system (CCS) creation of a cyber-physical system (CFS) "iPhone – Wi-Fi, Bluetooth – sensors" was created according to the standard ISO / IEC 15408 under the influence of threats, classified by the method STRIDE. The CCS system model of cyber-physical system was developed at cyberspace (CS) communication environment (CE) and physical space (PS) levels to provide security tasks – confidentiality (C), integrity (I), accessibility (Ac), observability (O), assuredness (As) under the proposed approach. Technologies of CPS information protection from STRIDE threats was analyzed according to security tasks.

Keywords: *cyber-physical system, complex security system, approach, system model, threats, security profiles, information protection technologies.*