**УДК 004.056**

**В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець**
Національний університет “Львівська політехніка”,
кафедра захисту інформації

# КВІНТЕСЕНЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КІБЕРФІЗИЧНОЇ СИСТЕМИ



**Подано квінтесенцію інформаційної безпеки (ІБ) кіберфізичних систем (КФС), яка: розгорнута на рівні парадигми та концепції побудови багаторівневої комплексної системи безпеки (КСБ) КФС і універсальної платформи КСБ у просторі “загрози – профілі – інструментарій”; реалізована у частині інтегральної моделі КСБ кіберфізичної системи “iPhone – Wi-Fi, Bluetooth – давачі” та криптографічного захисту безпровідного комунікаційного середовища КФС на основі блокового шифрування даних за алгоритмом “Калина”. Використання такого базового підходу до забезпечення ІБ КФС дасть змогу створити високоефективні технології інформаційної безпеки як кожного з сегментів КФС – кібернетичного простору (КП), комунікаційного середовища (КС), фізичного простору (ФП), так і трирівневої структури загалом.**

**Ключові слова: інформаційна безпека, кіберфізична система, парадигма, концепція, універсальна платформа, інтегральна модель, криптографічний захист.**

**The quintessence of an information security (IS) of cyber-physical systems (CPS) was presented, which is deployed on the level of complex security system (CSS) creation paradigm and conception as well as the CSS universal platform in the field “threats – profiles – tools”; it is also implemented in the part of CSS integral model of cyber-physical system “iPhone – Wi-Fi, Bluetooth – sensors” and cryptographic protection of CPS wireless communication environment based on block data encryption of algorithm “Kalyna”. Use of such basic approach and three-level CPS will allow creating of high effective information security technologies of each CPS segments – cyberspace (CS), communication environment (CE), physical space (PS) as well as the whole three-level structure.**

**Key words: information security, cyber-physical system, paradigm, concept, universal platform, integrated model, cryptographic protection.**

## Вступ

Стратегія кібернетичної безпеки України та Стратегія кібербезпеки Європейського Союзу, Загальне положення про захист даних (ЄС) спрямовані на розроблення підходів до забезпечення кібернетичного захисту об’єктів інформаційної інфраструктури суспільства та кібернетичної стійкості й безпеки інформаційно-комунікаційних та кіберфізичних систем [1–3].

Кіберфізичні системи є провідними у частині розроблення новітніх технологій та застосування у різних предметних сферах у контексті ефективного виконання обчислювальних задач під час взаємодії з фізичним простором та прийняття рішення щодо управління об’єктами та процесами [4]. Активно обговорюються напрями застосування КФС у контексті: 1) створення інтелектуального виробництва, інтелектуального енергопостачання, інтелектуальних споруд, транспорту та систем оборони; 2) формування інтернету речей як мережі фізичних об’єктів з вбудованими давачами для реєстрації та передавання даних про стан різнорідних об’єктів, середовища та структури взаємодії “об’єкт – середовище”. Перспектива сьогодні за: інтернетом загалом як комплексною системою – людей, процесів, даних, технічних пристроїв з метою формування необхідного та ефективного інформаційного рівня мережевих з’єднань, зокрема промисловим інтернетом як складною самоконфігурованою адаптивною системою мереж давачів та розумних об’єктів, призначення яких полягає у з’єднанні усіх речей, зокрема побутових і

промислових об’єктів. У сучасній інфраструктурі суспільства актуальним стає проектування інтернету чого завгодно як єдиної програмної екосистеми, що підтримує комплекс показів у динамічному режимі: усіх давачів, системних станів, експлуатаційних умов, контекстів даних. Ефективне функціонування інтелектуальних об’єктів у предметних сферах забезпечують КФС, структурований інтернет речей на рівні комунікаційного середовища. Інтернет речей як мережа мереж структурується рівнями: індивідуальних мереж; з’єднаних мереж, що забезпечують зв’язок між індивідуальними мережами; мережі зв’язку із системами безпеки та керування. Функціональність інтернету речей: масштабованість, доступність, керованість, управління даними, безпека, зручність користування. Відповідно актуальною проблемою у галузі інформаційної безпеки є розроблення стратегії забезпечення захищеного функціонування усіх рівнів, компонент та взаємозв’язків прикладних КФС у площинах кібернетичного і фізичного просторів та комунікаційного середовища.

Основні компоненти КФС розподілені в КП, КС, ФП, що зумовлює багаторівневість та вимагає гарантування безпечної інформаційної взаємодії рівневих та міжрівневих компонент КФС для виконання функціональних задач із даними: контроль/ обробка – передавання/приймання – управління. Функціонування КФС як складової кібернетичного простору України повинно бути безпечним, а також відповідати вимогам убезпечення від кібернетичних, комунікаційних, фізичних загроз. У цьому напрямі в Україні використовується стандарт ISO/IEC 15408 [5], ідеологія якого спрямована на безпекову структуру “загрози – послуги – механізми” через взаємозв’язок профілів (задач) безпеки інформаційних та комунікаційних систем: конфіденційність (К), цілісність (Ц), доступність (Д), спостережуваність (С), гарантії (С).

***Постановка завдання:*** розроблення концепції побудови комплексної системи безпеки КФС у контексті інтеграції рівнів і, на цій основі, створення моделі інформаційно-технічного стану КФС у функціональному просторі, яка уможливить побудову КСБ кіберфізичної системи будь-якої конфігурації за універсальною структурою інтеграції рівнів “КП – КС – ФП” відповідно до моделі загроз у межах забезпечення гарантоздатності КФС будь-якої предметної сфери.

***Мета роботи*** – формування квінтесенції інформаційної безпеки КФС на основі парадигми, концепції багаторівневої комплексної системи безпеки КФС; універсальної платформи та інтегральної моделі; розроблення КСБ кіберфізичної системи “iPhone – Wi-Fi, Bluetooth – давачі” відповідно до просторової моделі інформаційно-технічного стану та концепції забезпечення багаторівневої інформаційної безпеки КФС; створення алгоритмічно-програмного забезпечення криптографічного захисту даних у комунікаційному середовищі КФС на основі блокового алгоритму шифрування “Калина”.

**Розвиток підходів до побудови кіберфізичних систем та їхньої безпеки**

Кіберфізична система об’єднує кібернетичний та фізичний простори, інтегруючи обчислювальні та фізичні процеси за допомогою давачів і виконавчих пристроїв. Розвиток КФС розпочав Інститут стандартів і технологій ((NIST), США) (термін запропонувала Хелен Джилл, 2006). Актуальним є розвиток підходів до побудови кіберфізичних систем. У роботі [6] наведено архітектурні моделі КФС: 1) двокомпонентний взаємозв’язок фізичних і кібернетичних технологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем; 2) трикомпонентний взаємозв’язок фізичних, синергічних кібернетичних технологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем. Розглянуто принципи реалізації моделей КФС: системних (цілісних) зв’язків; специфікації на основі моделей; розроблення на основі платформ; обчислень у режимі реального часу; управління на основі подій; функціональності, орієнтованої на послуги; мінімальної інтрузивності. Розкрито технології реалізації трикомпонентної КФС: кіберкомпонента реалізується як програмні технології, технології передавання і зв’язку, мережеві технології; синергічна реалізується через технології цифрових мікросхем, сенсорні технології та мережі, міні-електромеханічні технології; фізична компонента реалізується як технології передових матеріалів, передові енергетичні та роботизовані технології. В праці [7] наведено засади проектування виробничих кіберфізичних систем на рівнях архітектури:

підключення, перетворення, кіберпізнання, конфігурації. У роботах [4, 8] запропоновано універсальну платформу для побудови прикладних кіберфізичних систем у контексті уніфікації міжрівневої взаємодії компонент КФС та уніфікації взаємодії компонент одного рівня: об'єкт дослідження та управління; організація вимірювально-обчислювальних процесів; збір/відбір, попередня обробка та передавання вимірювальної/управлінської інформації; захищений обмін, опрацювання та зберігання вимірювальної/управлінської інформації; користувач.

Розглянемо деякі аспекти розвитку досліджень із формування напрямів безпеки КФС та створення структур захисту інформації. Проектують структури "глибокого захисту" мереж прикладних КФС: план безпеки – розподілення мереж – захист периметра мережі – сегментація мережі – підвищення захищеності пристроїв – моніторинг/ оновлення [9]. У роботі [10] розглянуто підхід до аналізу виконаних та проведення нових досліджень у сфері безпеки кіберфізичних систем. Запропоновано платформу забезпечення безпеки КФС у контексті трирівневого захисту – цілі безпеки, підходи до забезпечення безпеки, безпека аплікацій [11]. Розроблено математичну платформу для безпечного створення та оцінювання КФС [12]. Проаналізовано сегменти забезпечення безпеки КФС – виявлення атак, моделювання атак, оцінювання та контроль рівня захищеності, формуються напрями досліджень безпеки КФС, серед яких: оцінювання ризиків, стратегії контратак, тестування та перевірка [13]. Розглянуто основні вектори атак на апаратне забезпечення КФС, які порушують конфіденційність, цілісність та автентичність, з урахуванням кібернетичних, фізичних аспектів [14].

**Парадигма створення багаторівневої КСБ кіберфізичних систем**

Багаторівнева КФС відповідно до структури "архітектура – функції – вимоги – застосування": фізичний простір, комунікаційне середовище, кібернетичний простір – контроль, обробка, управління – гарантоздатність, еталонна модель OSI, прецизійність давачів – масштабованість, реконфігурація у контексті багатофункціонального дослідження комплексу факторів впливу на різнорідні об'єкти предметних сфер. Структуру парадигми багаторівневої КСБ КФС подано на рис. 1.


*Рис. 1. Структура парадигми побудови багаторівневої КСБ кіберфізичних систем*

Згідно зі структурою парадигми, комплексні системи безпеки ФП, КС, КП як підсистеми захисту КФС передбачають: управління доступом; ідентифікацію та аутентифікацію;

криптографію; аудит; забезпечення цілісності, конфіденційності, аутентичності інформації. Система управління комплексною безпекою КФС ґрунтується на моделі “плануй – виконуй – перевіряй – дій” [15] та концепції “об’єкт – загроза – захист”.

**Концепція побудови багаторівневої інформаційної безпеки кіберфізичних систем**

Концепцію створення багаторівневої КСБ кіберфізичної системи наведено на рис. 2. Вона зумовлена структурою: класифікація загроз/атак – формування критеріїв захищеності – створення багаторівневої КСБ КФС – обґрунтування моделі політики безпеки – вибір методу оцінювання стану захищеності КФС [16, 17].

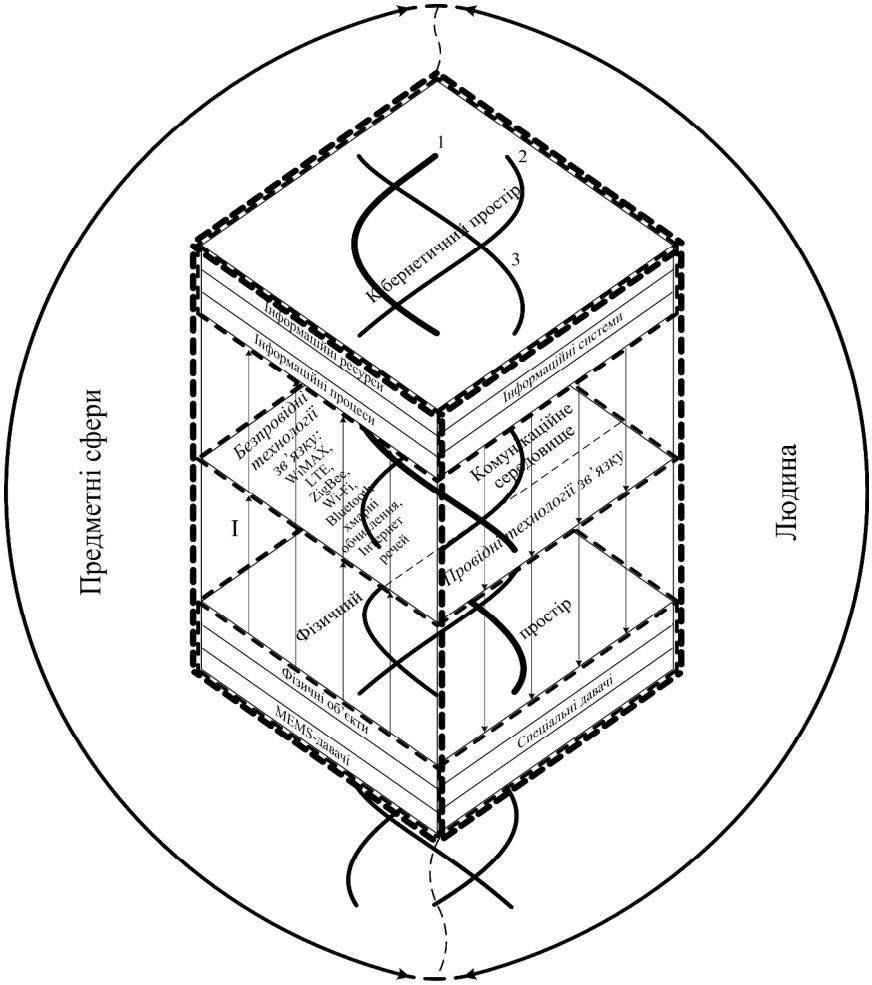


*Рис. 2. Структура концепції побудови КСБ кіберфізичних систем у контексті інтеграції рівнів*
*I ⟶ – інформація (відбір, управління); ▬ ▬ ▬ – КСБ КП, КС, ФП; ▬▬▬ – КСБ КФС;*
*1, 2, 3 – загрози відповідно для КП, КС, ФП*

Класифікація загроз/атак: загроз за ознаками; атак за кінцевим результатом, за способом здійснення; методика класифікації загроз STRIDE за категоріями (підміна об’єктів, модифікація даних, відмова від авторства, розголошення інформації, відмова в обслуговуванні, підвищення привілеїв) – створення моделі загроз “інформація / КФС – джерела виникнення загроз – способи реалізації загроз”. Критерії захищеності інформації в КФС: архітектура конфіденційності, цілісності, доступності, спостережності, гарантій. Цільова постановка задач безпеки спрямована на протидію загрозам безпеки та виконання вимог політики безпеки у сфері інформаційно-комунікаційних систем за допомогою розроблення комплексних систем захисту інформації, що працюють на виявлення, блокування і нейтралізацію інформаційних загроз.

Основою побудови багаторівневої КСБ КФС є: універсальна платформа “загрози – профілі – інструментарій”; інтегральна модель захисту інформації у КФС “рівень КФС – загроза STRIDE –

профіль безпеки – технологія безпеки"; методичні вказівки щодо розроблення технічного завдання на створення КСБ. Політика безпеки КФС ґрунтується на моделях та критеріях вибору відповідних методів і засобів захисту інформації. З метою оцінювання рівня захищеності КФС використовують уніфіковані методи забезпечення гарантоздатності [10].

**Універсальна платформа створення комплексної системи безпеки КФС**

Структуру платформи створення КСБ подано у просторі "загрози: STRIDE – профілі: конфіденційність, цілісність, доступність, спостережність, гарантованість – інструментарій: механізми, технології безпеки" (рис. 3). Вихідним етапом створення КСБ є обґрунтування вибору профілів безпеки КФС.

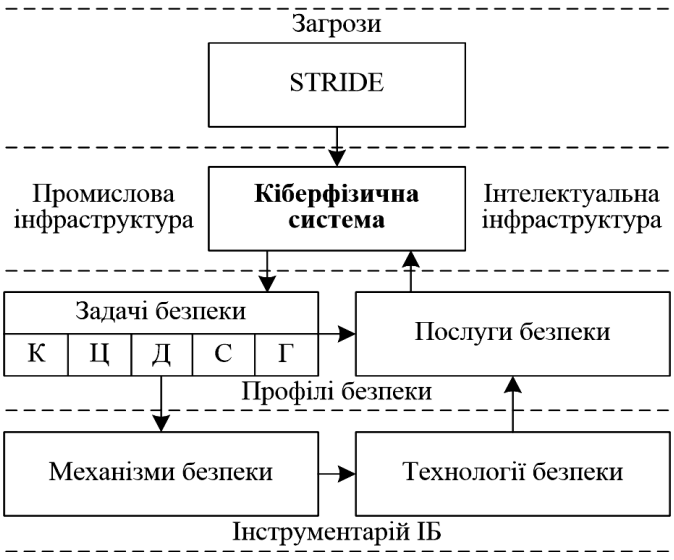


*Рис. 3. Універсальна платформа створення КСБ КФС у просторі "загрози – профілі – інструментарій"*

*Конфіденційність даних і системної інформації* полягає у тому, що інформацію не зможе отримати неавторизований користувач під час її зберігання, обробки і передавання.

*Цілісність даних* – їх не зможе модифікувати неавторизований користувач/процес під час їх зберігання, передавання і оброблення; *системи*, будь-який компонент якої неможливо видалити, модифікувати/додати, обійшовши або порушивши політику безпеки.

*Доступність систем, даних, ресурсів* – користувач (суб'єкт, процес) має відповідні права, може використати ресурс відповідно до правил, встановлених політикою безпеки, не чекаючи довше від заданого проміжку часу. Доступність спрямована на підтримання системи в працездатному стані, що забезпечує своєчасне і точне її функціонування через механізми відхилення: умисних/неумисних загроз, неавторизованого видалення даних, необґрунтованої відмови в доступі до послуги, спроб використання системи і даних у недозволених цілях.

*Спостережність* – реалізація можливості системи реєструвати будь-яку діяльність користувачів/процесів, використання пасивних об'єктів та встановлення ідентифікаторів, причетних до певних подій користувачів/процесів, щоб не допустити порушення політики безпеки. Реалізується через: механізми причетності, методи примусу, локалізацію несправностей, виявлення вторгнень, відновлення дій тощо.

*Гарантованість* – сукупність вимог, що становлять деяку шкалу оцінки для визначення міри упевненості у реалізації: функціональних вимог; організаційно-технічних заходів; захисту від умисних помилок користувачів/програмного забезпечення; достатньої стійкості до умисного проникнення та використання обхідних шляхів [5].

Щоб забезпечити вибрані профілі безпеки, КФС формують відповідні послуги безпеки – опорні; запобігання; виявлення порушень і відновлення безпеки. Інструментарієм створення КСБ є

механізми (загальні, спеціальні) та технології (методи і засоби) безпеки, які розробляються відповідно до послуг і завдань безпеки та забезпечують захист інформації на кожному рівні КФС та відповідно захищений міжрівневий обмін.

### Інтегральна модель комплексної системи безпеки КФС "iPhone – Wi-Fi, Bluetooth – давачі"

Інтегральну модель комплексної системи безпеки кіберфізичної системи "iPhone – Wi-Fi, Bluetooth – давачі" подано на рис. 4. Системна модель КСБ кіберфізичної системи складається із підсистем – комплексних систем безпеки КП, КС та ФП, що орієнтовані на забезпечення завдань безпеки процесів відбору, обробки, збереження, передавання даних.

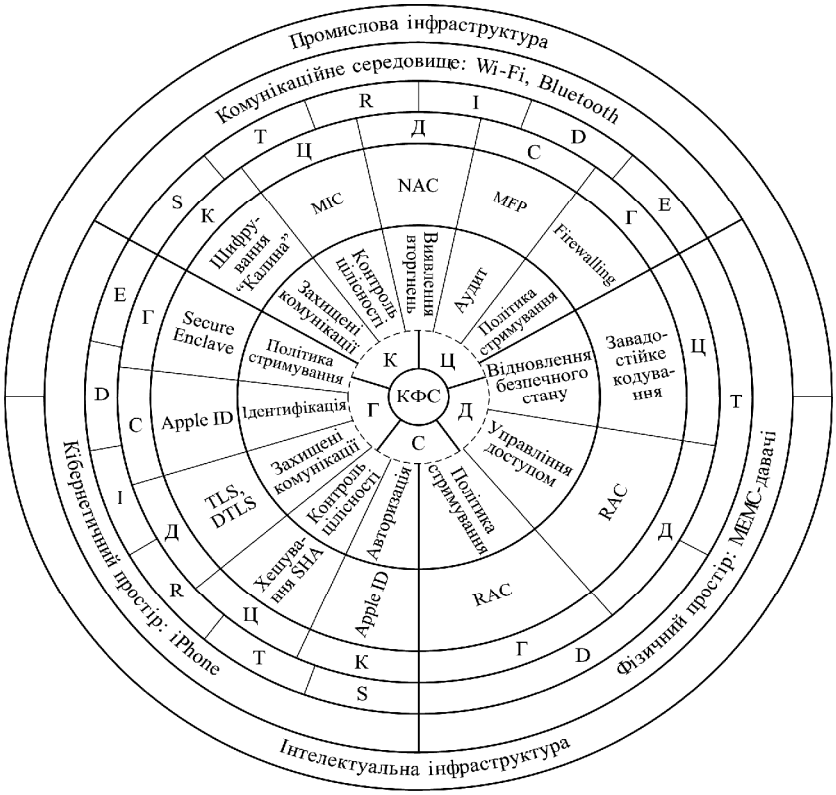


*Рис. 4. Інтегральна модель комплексної системи безпеки КФС "iPhone – Wi-Fi, Bluetooth – давачі"*

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 найхарактерніші загрози для КФС такі: 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/недосконалість 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, у який входять MEMC-давачі: Ц – відновлення безпечного стану – завадостійке кодування; Д – управління доступом – RAC; Г – політика стримування – RAC.

У табл. 1 наведено функціональну структуру КСБ КФС “загрози – профілі – технології захисту” відповідно до підходу та системної моделі.

*Таблиця 1*

**Комплексна система безпеки КФС у просторі “загрози – профілі – технології”**

| Задача безпеки/ стандартизація | Структура КФС: загрози – задача безпеки/технології захисту інформації | | |
|---|---|---|---|
| | КП / STRIDE | КС / STRIDE | ФП / TD |
| 1 | 2 | 3 | 4 |
| Конфіденційність | • SSL, VPN/несанкціонований віддалений доступ (I);<br>• ARM’s Execute Never/несанкціоноване виконання програмного забезпечення (I);<br>• оновлення ПЗ/використання вразливостей операційної системи (E) | • IPSEC/перехоплення пакетів (I);<br>• VPN/несанкціоноване збирання інформації про мережу (I);<br>• шифрування кодів доступу/перехоплення кодів доступу (S) | – |
| Цілісність | • захисне кодування/модифікація кодів доступу (T);<br>• низькорівневе шифрування AES-256/Jailbreak (T);<br>• сертифікація ОС/несанкціоноване знищення даних (T) | • IPSEC/маніпуляція бітами (атаки bit-flipping) (T);<br>• моніторинг підключень до мережі/виведення з ладу сеансових шлюзів (T);<br>• хешування/виникнення помилок у потоці даних (T) | • механізм здійснення контрольних вимірювань/ модифікація показів (T) |
| Доступність | • ланцюг довіреного завантаження пристрою/експлойти завантажувача системного ядра (D);<br>• сертифікація Apple Root/експлойти ядра системи (D);<br>• Apple Sandbox/несанкціонований запуск функції блокування пристрою (D) | • фільтрування пакетів/атаки DoS, DDoS (D);<br>• обмеження доступу до елементів мережі/виведення з ладу елементів мережі (D);<br>• періодичне тестування мережі/помилки мережі (D) | • дублювання давача/перебої електроживлення (D);<br>• аварійне вимкнення/ перевищення порогових значень (D);<br>• самодіагностика/ відмови (D) |
| Спостережуваність | • технологія фіксації дій користувача/заміна цифрових сертифікатів, підписів (R);<br>• сертифікація програм/маскування шкідливого програмного забезпечення (R);<br>• дактилоскопічний давач/ несанкціоновані покупки через програми (R) | • віддалене логування / маскування налаштувань (R);<br>• ідентифікація, аутентифікація користувачів/несанкціоноване використання ресурсів мережі (R);<br>• обмеження доступу до облікових даних та послуг/ несанкціоноване використання/зміна послуг (R) | – |

*Продовження табл. 1*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Гарантованість | • сертифікація програм та пристроїв/соціальна інженерія (S);<br>• сертифікація прошивки SHSH/підміна об'єктів (S);<br>• періодичне оновлення операційної системи та програм/використання вразливостей операційної системи (E) | • ідентифікація обладнання/підміна пристроїв (атака man-in-the-middle) (S);<br>• багатофакторне підтвердження змін/несанкціонована зміна статусів підключення (E);<br>• ідентифікація учасників сеансу/несанкціонована зміна прав доступу (E); | • механізм здійснення контрольних вимірювань/ модифікація показів (T);<br>• самодіагностика/ апаратні відмови (D) |
| Стандарти | • NIST Special Publication 800-164. 2012. Guidelines on hardware-rooted security in mobile devices (draft);<br>• NIST Special Publication 800-124. 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise;<br>• Government Mobile and Wireless Security Baseline. 2013;<br>• Mobile-Computing Device (MCD) Standards and Guidelines. A Mandatory Reference for ADS Chapter 545 2014 | • ДСТУ ISO/IEC 7498-3:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 3. Найменування та адресація.<br>• ISO/IEC 27033-3:2010. Information technology. Security techniques. Network security. Reference networking scenarios.<br>Threats, design techniques and control issues;<br>• ISO/IEC 27033-4:2014. Information technology. Security techniques. Network security | • IEEE 2700-2014 Standard for Sensor Performance Parameter Definitions;<br>• IEC 62047-Series. Part 1-22. Micro-Electromechanical Devices – MEMS<br>• IEEE 1451 Smart Transducer Interface Standards<br>• IEEE 451 Proposed Recommended Guide for Specification of Signal Sources |

**Криптографічний метод захисту комунікаційного середовища КФС**

З метою підвищення стійкості криптографічного захисту інформації у КФС запропоновано застосовувати блоковий алгоритм "Калина", який може слугувати підґрунтям адаптації шифрування/дешифрування даних у технологіях безпровідного зв'язку, що формують сегмент КП кіберфізичної системи.

Алгоритм "Калина" функціонує на основі змінних розміру блока та довжини ключа (128, 256, 512). Шифр має SPN-структуру (Rijndael-подібну) з підвищеним розміром матриці MDS, новий набір з чотирьох різних S-блоків, до і після відбілювання, використовуючи суму за модулем $2^{64}$ і нову конструкцію розкладу ключів. Стандарт "Калина" забезпечує достатній запас криптостійкості – 6, 7 та 9 циклів для 128-, 256- та 512-бітового блоків відповідно за 10, 14 та 18 циклів шифрування. Для оптимізованих версій програмної реалізації на 64-бітових платформах алгоритм демонструє вищу швидкодію, ніж аналоги: для 128-бітового ключа – перевага 86–143 Мбіт/с порівняно з AES; для 256-бітового ключа – перевага 4 % порівняно з AES; швидкодія за розміру ключа 512 бітів – на рівні 256-бітової версії AES. Висока криптостійкість та швидкодія алгоритму блокового шифрування "Калина" уможливлюють його ефективне застосування у технологіях безпровідного зв'язку в складі кіберфізичної системи.

Розглянемо криптографічне перетворення на основі стандарту "Калина" [18]. Базове перетворення шифрування $T_{l,k}^{(K)}$ визначається так:

$$T_{l,k}^{(K)} = h_l^{(K_t)} \mathbf{o} y_l \mathbf{o} t_l \mathbf{o} p_l' \mathbf{o} \prod_{n=1}^{t-1} (k_l^{(K_n)} \mathbf{o} y_l \mathbf{o} t_l \mathbf{o} p_l') \mathbf{o} h_l^{(K_0)},$$

де $K$ – ключ шифрування довжини $k$ бітів; $h_l^{(K_n)}$ – функція суми за модулем $2^{64}$ внутрішнього стану та раундового ключа $K_n$ ; $p_l'$ – шар взаємно однозначного відображення, що обробляє вектори байтів (елементів $V_8$). Застосовує шар S-блоків. Кожен елемент $g_{i,j} \in V_8$ матриці вхідного стану замінюється на $p_{i \bmod 4}(g_{i,j})$, де $p_s \in V_8$ **а** $V_8$, $s \in \{0,1,2,3\}$ є визначеними замінами (S-блоками); $t_l$ – перестановка елементів $g_{i,j} \in GF(2^8)$ вхідного стану шифру. Виконує циклічний зсув вправо для рядків матриці внутрішнього стану $G = (g_{i,j})$. Кількість зсунутих елементів залежить від номера рядка $i \in \{0,1,...,7\}$, розміру блока $l \in \{128,256,512\}$ і розраховується за формулою $d_i = \left[\frac{i \cdot l}{512}\right]$; $y_l$ – лінійне перетворення елементів вхідного стану в скінченному полі. Під час цього перетворення кожен елемент $g_{i,j} \in V_8$ матриці внутрішнього стану $G$ подається як елемент скінченного поля $GF(2^8)$, сформований незвідним многочленом $\Psi(x) = x^8 + x^4 + x^3 + x^2 + 1$ або $0\text{x}11D$ у шістнадцятковій формі. Елементи нової матриці стану $W = (w_{i,j})$ обчислюють у $GF(2^8)$ за формулою $w_{i,j} = (v >>> i) \otimes G_j$, де $v = (0\text{x}01, 0\text{x}01, 0\text{x}05, 0\text{x}01, 0\text{x}08,\ 0\text{x}06, 0\text{x}07, 0\text{x}04)$ – вектор, який формує циркулянтну матрицю з властивістю MDS, $G_j$ – $j$-й стовпець матриці стану $G$; $k_l^{(K_n)}$ – функція суми за модулем 2 раундового ключа $K_n$ та матриці стану. У функціях $p_l'$, $t_l$ та $y_l$ вхідний аргумент $x \in V_l$ і вихідне значення $c(x) \in V_l, c \in \{p_l', t_l, y_l\}$ подано як матриці розміру $8 \times c$.

Базове перетворення дешифрування $U_{l,k}^{(K)}$ визначається так:

$$U_{l,k}^{(K)} = -1h_l^{(K_0)} \mathbf{0} \prod_{n=t-1}^{1} (-1p_l' \mathbf{0} -1t_l \mathbf{0} -1y_l \mathbf{0} k_l^{(K_n)}) \mathbf{0} -1p_l' \mathbf{0} -1t_l \mathbf{0} -1y_l \mathbf{0} -1h_l^{(Kt)},$$

де $K$ – ключ шифрування довжини $k$ бітів; $-1h_l^{(K_n)}$ – функція віднімання за модулем $2^{64}$ раундового ключа $K_n$ від внутрішнього стану; $-1y_l$ – зворотне лінійне перетворення елементів вхідного стану в скінченному полі. Кожен елемент $g_{i,j} \in V_8$ матриці внутрішнього стану $G$ подається як елемент скінченного поля $GF(2^8)$, сформований незвідним многочленом $\Psi(x) = x^8 + x^4 + x^3 + x^2 + 1$ або $0\text{x}11D$ у шістнадцятковій формі. Кожен елемент нової матриці стану $-1W = (-1w_{i,j})$ обчислюють у $GF(2^8)$ за формулою $-1w_{i,j} = (-1v <<< i) \otimes G_j$, де $-1v = (0\text{x}AD, 0\text{x}95, 0\text{x}76, 0\text{x}A8,\ 0\text{x}2F, 0\text{x}49, 0\text{x}D7, 0\text{x}CA)$ – вектор, який формує циркулянтну матрицю з властивістю MDS, $G_j$ – $j$-й стовпець матриці стану $G$. $-1t_l$ – зворотна перестановка елементів $g_{i,j} \in GF(2^8)$ вхідного стану шифру. Виконує циклічний зсув вліво для рядків матриці внутрішнього стану $G = (g_{i,j})$. Кількість зсунутих елементів залежить від номера рядка $i \in \{0,1,...,7\}$, розміру блока $l \in \{128,256,512\}$ і розраховується за формулою $d_i = \left[\frac{i \cdot l}{512}\right]$; $-1p_l'$ – шар зворотного взаємно однозначного відображення (шар зворотного S-блока), що обробляє вектори байтів (елементів $V_8$). Застосовує шар зворотних S-блоків. Кожен елемент $g_{i,j} \in V_8$ матриці вхідного стану замінюється на $-1p_{i \bmod 4}(g_{i,j})$, де $-1p_s \in V_8$ **а** $V_8$, $s \in \{0,1,2,3\}$ є

визначеними замінами (зворотними S-блоками); $k_l^{(K_n)}$ – функція суми за модулем 2 раундового ключа $K_n$ та матриці стану (інволютивна функція). Алгоритм “Калина” реалізовано у режимі ECB з розмірами ключа та блока 512 бітів засобами мови програмування Java, що забезпечує максимальний рівень криптостійкості. На рис. 5 наведено блок-схеми роботи програми для шифрування даних та генерації раундових ключів відповідно.

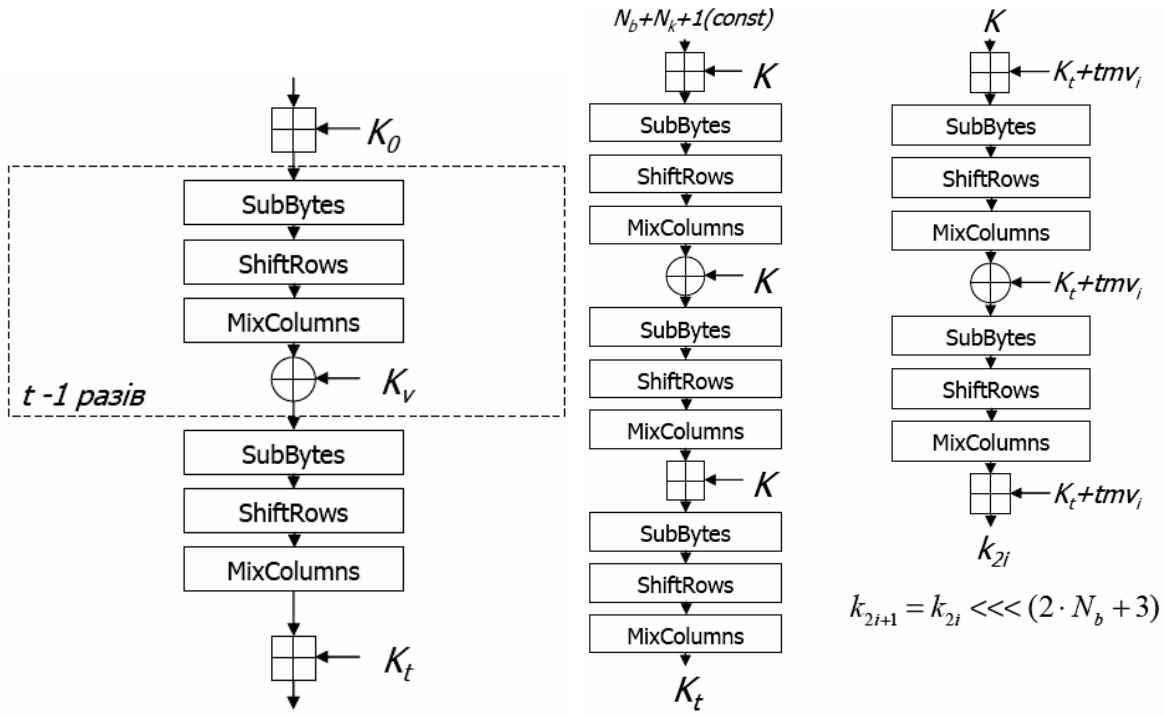


*Рис. 5. Блок-схеми шифрування даних та генерації раундових ключів*:
*SubBytes – операція заміни байтів, ShiftRows – операція зсуву рядків матриці,*
*MixColumns – операція змішування стовпців*

На рис. 6 наведено результат виконання програми.

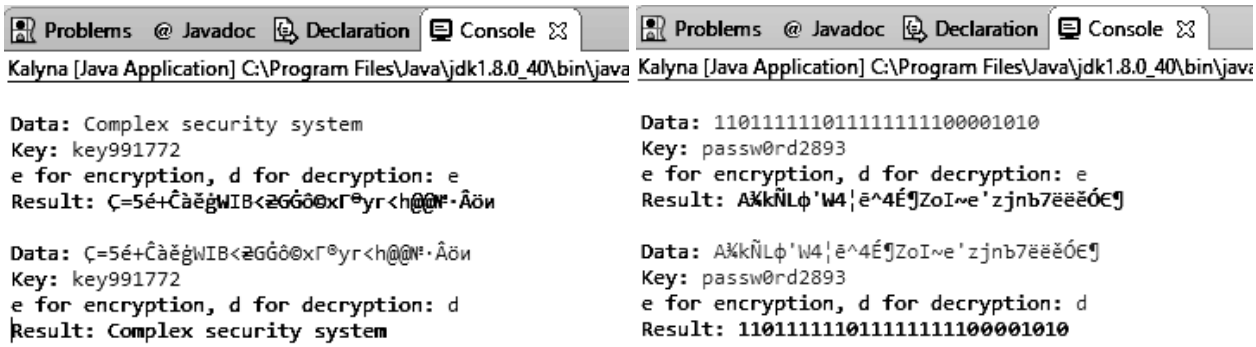


*Рис. 6. Результат виконання програми*

## Висновки

Висвітлено квінтесенцію інформаційної безпеки КФС на основі розробленої концепції побудови КСБ КФС та універсальної платформи створення КСБ, яка, відповідно до уніфікованої структури “загрози – профілі – інструментарій”, трансформується у відповідні моделі інформаційної безпеки КП, КС, ФП. Як приклад реалізації концепції та універсальної платформи створення КСБ подано інтегральну модель системи безпеки КФС “iPhone – Wi-Fi,

Bluetooth – давачі", згідно з якою розкрито криптографічний метод захисту інформації у безпровідному КС на рівні програмної реалізації алгоритму шифрування даних "Калина" засобами мови програмування Java.

*1. Проект Стратегії кібернетичної безпеки України [Електронний ресурс]. – Режим доступу: http://www. niss. gov. ua/public/File/2013_nauk_an_rozrobku/kiberstrateg. pdf. 2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. – Brussels, 7.2.2013 [Online resource]. – Access at: http://www. eeas. europa. eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en. pdf. 3. General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [Online resource]. – Access at: http://ec. europa. eu/justice/data-protection/reform/files/regulation_oj_en. pdf. 4. Мельник А. О. Інтеграція рівнів кіберфізичної системи / А. О. Мельник // Вісник Національного університету "Львівська політехніка", Комп'ютерні системи та мережі. – 2015. – № 830. – С 61–68. 5. Information technology. Security techniques. Evaluation criteria for IT security. Part 1–3: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008. – [Active from 2009.01.01]. – Switzerland: ISO copyright office, 2009. – 56, 161, 150 p. 6. Imre Horváth, Bart H. M. Gerritsen. Cyber-physical systems: concepts, technologies and implementation principles // 9th International Symposium on Tools and Methods of Competitive Engineering (TMCE), May 7 – 11, 2012, Karlsruhe, Germany. 7. Jay Lee, Behrad Bagheri, Hung-An Kao. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), University of Cincinnati, Cincinnati, OH, United States, 2014. 8. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Нац. ун-ту "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 154–161. 9. National Institute of Standards and Technology Special Publication 800-53. – NIST SP 800-53 – 2011. – 155 p. 10. Yuriy Zacchia Lun, Alessandro D'Innocenzo, Ivano Malavolta [and others] Cyber-Physical Systems Security: a Systematic Mapping Study // ArXiv. – 2016. – 32 p. 11. Tianbo Lu, Jinyang Zhao, Lingling Zhao [and others] Towards a Framework for Assuring Cyber Physical System Security // International Journal of Security and Its Applications. – Vol. 9, No. 3. – 2015 – P. 25–40. 12. Jeff Hughesa, George Cybenkob Three Tenets for Secure Cyber-Physical System Design and Assessment // Cyber Sensing. – 2014. – Vol. 9097. – 15 p. 13. Guangyu Wu, Jian Sun, Jie Chen A survey on the security of cyber-physical systems // Control Theory and Technology. – 2016. – Vol. 14, No. 1. – P. 2–10. 14. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – [Active from 2013.10.01]. – Switzerland: ISO copyright office, 2013. – 23 p. 15. Francesco Regazzoni, Ilia Polian Securing the hardware of cyber-physical systems // 22nd Asia and South Pacific Design Automation Conference (ASP-DAC). – 16–19 Jan. 2017. – P. 194–199. 16. Space product assurance. Methods and techniques to support the assessment of software dependability and safety. – ECSS-Q-80-03, 2006. – 122 p. 17. Information processing systems. Open Systems Interconnection. Basic Reference Model – Part 2: Security Architecture, – ISO 7498-2:1989. – 32 p. 18. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624: 2014. – [Чинний від 2015-07-01]. – К: Держспоживстандарт, 2016. – 117 с.*