УДК 621.396.49:004.056 **doi: 10.32620/reks.2020.4.07**

В. Я. ПЕВНЄВ, В. В. ТОРЯНИК, В. С. ХАРЧЕНКО

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна

КІБЕРБЕЗПЕКА БЕЗПРОВОДОВИХ СМАРТ-СИСТЕМ: КАНАЛИ ВТРУЧАНЬ ТА РАДІОЧАСТОТНІ ВРАЗЛИВОСТІ

Предметом *даного дослідження є кіберуразливість радіочастотної технології інформаційно-управляючої взаємодії в безпроводових смарт-системах (БСС). БСС – це кіберфізічні системи, що функціонують у рамках моделі OSI. Специфіка і спеціалізація таких систем визначається радіотехнологіями фізичного рівня, наприклад, видами БСС є Інтернет Речей (IoT, зокрема, медичний IoMT, Інтернет Дронів (IoD)), системи авіамоніторингу ADS-B і управління трафіком ATM, а в перспективі - системи Інтернету Всього (IoE).* ***Метою*** *є аналіз радіочастотних параметрів інформаційно-управляючої взаємодії в БСС для виявлення їх потенційних кіберуразливостей.* ***Задачі****: узагальнити та систематизувати фізичні і функціональні параметри безпроводових технологій у діапазонах ISM (Industrial Scientific & Medical Band) і SRD ((Short range devices) істотні з точки зору кіберуразливості каналів БСС, включаючи також навігаційні технології, що використовуються. Проаналізувати тренди і методи успішних кібератак на БСС, виділити такі, що були реалізовані через радіочастотне втручання. Виконати експертні оцінки потенційної кіберуразливості БСС в залежності від їх архітектури та області застосування.* ***Методами****, що використовуються є: аналіз трендів відомих радіочастотних інцидентів і експертні оцінки кіберуразливості інформаційно-управляючих каналів БСС. Одержані наступні* ***результати****. Проаналізовано 12 актуальних радіотехнологій БСС. Типізовані 6 видів можливих радіочастотних кібератак на БСС. Виконано експертне оцінювання ймовірності використання уразливостей за діапазонами, радіотехнологіями та видами атак. Показана особлива небезпека високотехнологічних цільових APT-атак, а також висока потенційна радіочастотна уразливість БСС як кіберфізичних систем. Особливо відзначена кіберуразливість авіаційних систем ADS-B.* ***Висновки****. Наукова новизна отриманих результатів полягає у наступному: виявлено тренд зниження вартості APT-атак і зростання ймовірності їх реалізації за допомогою нових можливостей SDR-технології (Software Defined Radio - програмно визначаєме радіо). Проаналізована можливість керованої SDR-компрометації параметрів безпеки каналів БСС в будь-якому радіодіапазоні. Запропоновано перспективний напрямок досліджень SDR-пентестінг БСС.*

Ключові слова: *безпроводова смарт-система; радіочастотне інформаційно-управляюча взаємодія; радіочастотна кіберуразливість; авіакібербезпека; програмно-визначаєме радіо; SDR-пентестінг.*

Вступ

Сучасний рівень розвитку інформаційно-комп'ютерних технологій дозволяє створювати новий клас управляючих інтелектуальних (смарт) систем будь-яких рівнів складності і інтеграції - від розумних датчиків (IoT) до систем автоматичного управління авіатрафіком (ATM). Основою функціональних можливостей таких систем є технології розподілених обчислень, засновані на безпроводовому (радіочастотному) обміні даними.

Узагальнюючи, введемо поняття безпроводової смарт-системи (БСС). БСС - це комп'ютерні системи обробки інформації та управління, що динамічно та всебічно розвиваються, базуються на мобільних безпроводових комунікаціях і всепроникаючій автоматизації та застосовуються у різних галузях.

Специфіка і спеціалізація таких систем заснована на прогресі у технологіях фізичного рівня, так, наприклад, можна прослідкувати деякі етапи їх еволюції: відомі системи Інтернету Речей (IoT, зокрема, медичних IoMT), Інтернету Дронів (IoD, системи авіамоніторінгу) і, логічно, в перспективі - системи Інтернету Всього (IoE).

Таким чином, до БСС можуть бути віднесені будь-які розподілені комп'ютерні, інформаційні та / або управляючі системи такої архітектури:

- джерела інформації (датчик фізичного параметра, фотокамера, оператор);
- локальні обробники інформації (процесор, кодер);
- канали радіопередачі даних (IEEE 802.xx, пропрієтарні, тощо);
- віддалені сховища даних (хмарні сервіси);
- одержувачі інформації (диспетчери, оператори, виконавчі пристрої, авіоніка);
- канали радіопередачі команд управління (IEEE 802.xx, пропрієтарні, тощо);

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

– виконавчі пристрої (оператори, пілоти, приводи і т.п.).

Інакше кажучи, БСС - це кіберфізічна система, що працює в рамках моделі OSI [1, 2]. З точки зору кібербезпеки БСС інтерес представляє в першу чергу нижній фізичний рівень моделі OSI. Як відомо, радіочастотні канали БСС є кіберуразливими [2 - 4].

Конкретними видами БСС, що представляють інтерес для даного дослідження, є радіочастотна уразливість, зокрема, навігаційних GPS-систем [5], авіаційних систем залежного спостереження-мовлення ADS-B [6-8], і навіть систем моніторингу критичних інфраструктур [4].

1. Постановка задачі

Актуальність даного дослідження обумовлена стійкою тенденцією запровадження у всіх галузях діяльності смарт-систем з безпроводовою архітектурою. Кіберуразливість таких рішень є системною, розроблення і впровадження методів і засобів кіберзахисту БСС становить суттєву науково-технологічну проблему. Зокрема, предметом даного дослідження є радіочастотна кіберуразливість (РЧКУ) технологій інформаційно-управляючої взаємодії в безпроводових смарт-системах. Під РЧКУ будемо розуміти потенційні можливості, методи та засоби несанкціонованого втручання у роботу БСС, які ґрунтуються на фізичних принципах та специфіці системних радіотехнологій, що застосовуються. Важливість системного аналізу РЧКУ зумовлена новими можливостями, що надає технологія програмно визначаємого радіо (SDR).

Цілями даного дослідження є:

– аналіз актуальних неліцензованих радіодіапазонів і технологій, що є придатними для використання у БСС;

– систематизація фізичних і функціональних параметрів інформаційно-управляючої взаємодії в БСС;

– аналіз і типізація трендів щодо кібератак на БСС;

– виявлення та аналіз потенційних радіочастотних кіберуразливостей БСС;

– аналіз можливостей несанкціонованої радіовзаімодії з БСС методами програмно визначаємого радіо (SDR).

2. Огляд технологій радіочастотної інформаційно-управляючої взаємодії в безпроводових смарт-системах

Наведемо короткий огляд технологій радіочастотної інформаційно-управляючої взаємодії в БСС з акцентом на радіочастотну кіберуразливість. Особливий інтерес представляє так званий ISM-діапазон (Industrial Scientific & Medical Band) [9, 10].

ISM-діапазон - це частина радіочастотного спектру загального призначення, що використовується без ліцензування. Однак, пристрої ISM-діапазону, що розробляються, повинні відповідати певним регіональним нормам, які встановлюються регулюючими органами для даної частини частотного спектра та географічного регіону.

У США норми встановлює Федеральна комісія із зв'язку (Federal Communication Commission, FCC), у Європі - Європейський інститут стандартів з телекомунікацій (European Telecommunication Standards Institute, ETSI), в Україні - Національна комісія з питань зв'язку та інформатизації (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, (НКЗІ). Нормуванню підлягають частотні плани і відповідні їм максимальні потужності радіовипромінювань [11].

Технологічними радіочастотними елементами БСС є так звані пристрої ближньої дії (Short range devices, SRD) [12], що забезпечують такі дистанційні інформаційно-управляючі функції БСС:

– контроль фізичного доступу;
– детектування руху і сигналізація;
– системи охоронного телебачення;
– безпроводове аудіо;
– промисловий контроль;
– локальні мережі;
– медичні імплантати;
– прилади обліку;
– дистанційне управління;
– радіочастотна ідентифікація;
– дорожня транспортна телематика;
– телеметрія.

Нижче узагальнено та систематизовано фізичні та функціональні параметри бездротових технологій ISM і SRD, істотні з точки зору радіочастотної кіберуразливості БСС.

Bluetooth

Це радіотехнологія низької потужності стандарту 802.15.1 (див. нижче). У ній використовується так званий нижній ISM-діапазон у межах 2,4…2,5 ГГц. У 2001 році деяким виробникам вдалося збільшити дальність зв'язку з 10 до 100 метрів.

Дана технологія базується на стандарті IEEE 802.15.1.Bluetooth, який дозволяє пристроям встановлювати зв'язок в діапазоні частот 2,4…2,4835 ГГц в радіусі від 1 до 10 м.

В стандарті Bluetooth доступні три рівня вихідної потужності. 1 мВт, 2,5 мВт і 100 мВт, що забезпе-

чує радіус дії близько 1 м, 10 м і 100 м відповідно [13].

802.xx

802.xx визначає радіотехнологію і групу стандартів, що розроблені спеціальним комітетом IEEE 802 (802.11 a, b, g, n, ac; 802.15) для організації локальних бездротових мереж (широко відомих як WiFi-мережі або WLAN), в тому числі і для IoT [9]. На фізичному рівні (табл.1) використовуються частотні діапазони 2,4; 3,6; 5, і 6 ГГц. Максимальна потужність випромінювання не перевищує 1 Вт, радіус впевненого прийому - близько 100 м. В Україні використання Wi-Fi без дозволу НКРЗІ можливе при потужності сигналу до 100 мВт на частоті 2,4 ГГц і до 200 мВт - на 5 ГГц за умов розташування антен усередині приміщення [10, 11].

Z-Wave

Це бездротова радіотехнологія, розроблена спеціально для дистанційного управління. Z-Wave є запатентованим безпроводовим протоколом зв'язку для домашньої автоматизації, зокрема, для контролю і управління на житлових і комерційних смарт-об'єктах. Технологія використовує малопотужні мініатюрні радіочастотні модулі, що вбудовуються в побутову електроніку і різні пристрої, такі як освітлення, опалення, контроль доступу, розважальні системи і також в побутову техніку.

На відміну від Wi-Fi і інших IEEE 802.11-стандартів передачі даних, призначених в основному для великих потоків інформації, Z-Wave працює в діапазоні частот до 1 ГГц. Вибір такого діапазону зумовлений відсутністю частотної оптимізації (на відміну від Wi-Fi) для передачі простих команд управління (наприклад, включити / виключити, змінити гучність, яскравість, тощо). Використання низького радіочастотного діапазону для Z-Wave також обумовлюється малою кількістю можливих тут джерел електромагнітних завад.

Також істотною перевагою пристроїв Z-Wave є мале споживання енергії, низька вартість їх виробництва та інтеграції в різні пристрої автоматики. У світі налічується понад 200 виробників Z-Wave чіпів і модулів, причому всі ці продукти сумісні між собою. Енергоефективність Z-Wave-рішень обумовлена стільниковою мережевою архітектурою (mesh), в якій кожен вузол або пристрій може приймати і передавати сигнали інших пристроїв мережі, використовуючи проміжні сусідні вузли.

Використовувана технологія Mesh – це самоорганізована мережа з маршрутизацією, залежною від зовнішніх факторів, наприклад, при виникненні перешкоди між двома найближчими вузлами мережі, сигнал переспрямовується через інші вузли мережі, що знаходяться в радіусі дії [14].

NFC

NFC (Near Field Communication) – радіотехнологія бездротової ближньої взаємодії, що забезпечує обмін даними між пристроями в радіусі близько 10 см, забезпечуючи їх роботу у безконтактному режимі, наприклад карти типу CmartCard. За технологією NFC працюють всі системи радіочастотної ідентифікації (RFID). Вони розроблені на основі стандартів ISO / IEC 14443, ISO / IEC 18000-3, що регламентують радіозв'язок в межах діапазону ISM.

Радіообмін здійснюється за допомогою електромагнітної індукції на частоті 13,56 МГц через рамкові антени в межах їх індуктивного зв'язку. При цьому активний пристрій, що опитує, активує і забезпечує енергією пасивний приймальний пристрій [15, 16].

LPD433

LPD433 (Low Power Device) - загальна назва неліцензованого діапазону 433,05 - 434,79 МГц для радіоперемовних, охоронних, телеметричних, медичних і радіокерованих пристроїв з максимальною дозволеною потужністю до 10 мВт [17].

PMR446

PMR446 (Private Mobile Radio) європейська аналогова безліцензійна система рухомого персонального радіозв'язку УКХ-діапазону. Використовує вісім каналів з частотною модуляцією в смузі 446…446,1 МГц з максимально дозволеною потужністю передавача 0,5 Вт.

Як і в більшості країн Європи, в Україні можливо вільне використання PMR446 за умови включення абонентських станцій в перелік радіоелектронних засобів, які не потребують отримання дозволів Українського державного центру радіочастот (УДЦР) на їх експлуатацію [18].

L-діапазон

L-діапазон використовується всіма супутниковими системами навігації, крім індійської системи GAGAN, що розробляється. Таким чином, в цьому діапазоні передаються сигнали [19]:

– американської системи супутникової навігації GPS на центральних частотах 1176,45 МГц (L5), 1227,60 МГц (L2), 1381,05 МГц (L3), і 1575,42 МГц (L1);

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

– європейської системи Galileo на частотах 1164…1214 МГц і 1563…1591 МГц для цивільного сигналу і 1260…1300 МГц для кодованого військового сигналу;

– російської системи ГЛОНАСС з частотним поділом з центральними частотами

1602 МГц + 0,5625n МГц (діапазон L1)
і 1246 МГц + 0,4375n МГц (діапазон L2),

де n позначає канал частоти супутника n = -7, -6, -5 ... 0, ..., 6 і кодовим поділом з центральною частотою 1202,25 МГц (діапазон L3), а також в перспективі – 1600,995 МГц (L1) і 1248,06 МГц (L2);

– китайської супутникової навігаційної системи BeiDou на частотах 1559,052…1591,788 МГц.

Також в цьому діапазоні працюють мобільні телефони стандарту GSM на частотах 800…900 і 1800…1900 МГц.

GPS

Систему GPS має сенс розглянути детально, оскільки вона є найрозповсюдженішою технологією геопозиціювання смарт-об'єктів. Супутникова навігаційна система (Global Position System, GPS) розроблена, реалізована і експлуатується Міністерством оборони США, при цьому в даний час доступна для використання в цивільних цілях як основна навігаційна система [20].

Основний принцип роботи системи - визначення місця розташування шляхом вимірювання моментів часу прийому синхронізованого сигналу від навігаційних супутників антеною споживача.

Для визначення власних тривимірних координат GPS-приймача потрібно мати чотири рівняння типу «відстань дорівнює добутку швидкості світла на різницю моментів прийому сигналу споживачем і моменту його синхронного випромінювання від супутників», тобто мати у полі зору мінімум чотири супутника. Супутники GPS транслюють сигнал із космосу і всі приймачі GPS використовують цей сигнал для обчислення свого положення в просторі за трьома координатам в режимі реального часу [21].

ADS-B

ADS-B (Automatic dependent surveillance-broadcast, АЗН-В – автоматичне залежне спостереження-мовлення) – радіотехнологія, що дозволяє і льотчикам в кабіні літака, і авіадиспетчерам в наземному пункті спостерігати рух повітряних суден (ПС) з більшою точністю, ніж це було доступно раніше, і отримувати поточну аеронавігаційну інформацію. ADS-B також передає льотчикам в режимі реального часу погодну інформацію.

Вважається, що таким чином надана інформація значно розширює обізнаність льотчика про поточну обстановку і в цілому підвищує безпеку польотів [22].

Доступ до ADS-B інформації безкоштовний і вільний для всіх через он-лайн сервіс flightradar24.com.

Система ADS-B має наступні параметри роботи:

– режим Mode-A – так званий вторинний радар (Secondary Surveillance Radar (SSR)), використовується як цивільними, так і військовими повітряними судами, забезпечує до 4096 ідентифікаційних кодів (код відповідача) і є найбільш поширеним і використовуваним режимом. Працює на частоті запиту 1030 МГц. У режимі Mode-A передаються дані про висоту, код відповідача і ICAO-код ПС, координати не передаються;

– режим Mode-S – є двочастотним, «слухає» на частоті запиту 1030 МГц, але «відповідає» на частоті 1090 МГц, модулюючи несучу сигналу DPSK для мінімізації перешкод іншим запитам Mode A; тільки в режимі Mode-S передаються поточні координати ПС.

Коли транспондер ПС отримує запит від наземного радара, він підтверджує отримання запиту випромінюванням фазово-імпульсно модульованого сигналу на частоті 1090 МГц. Незалежно від надходження запиту від наземного радара, приблизно кожну секунду ПС передає розширений пакет даних (так званий extended squitter).

ADS-B базується на системі GPS для визначення точних координат ПС в просторі і режимі реального часу. Ця інформація про розташування ПС комбінується з іншою інформацією, такою як тип повітряного судна, його номер, рейс, курс, курсова швидкість вертикальна швидкість і потім широкомовно передається приблизно кожну секунду.

Інші повітряні судна і наземні станції, що, також обладнані системами ADS-B, мають можливість в радіусі приблизно 150 миль приймати цю інформацію. Наземні станції комбінують інформацію, що прийнята від різних ПС з додатковою інформацією, отриманою від наземних радарів і ретранслюють такі дані для всіх повітряних суден в радіусі обслуговування.

Таким чином, при аналізі актуальних радіотехнологій інфокомунікаційного обміну у БСС систематизовані їх фізичні параметри, знання яких необхідно для дослідження системних радіочастотних кіберуразливостей БСС. Результати проведеного аналізу актуальних радіотехнологій БСС зведені в таблицю1.

Підсумовуючи зауважимо, що фізичні параметри радіотехнологій БСС укладаються у частотно-просторовий діапазон типової розмірності від $4*10^8$ до $1,6*10^9$ Гц та від 10^{-2} до $3*10^3$ м. Ці данні будуть використовуватися для планування подальшого дослідження функціональних уразливостей БСС.

Таблиця 1

Фізичні параметри радіотехнологій БСС

Радіотехнологія	Діапазон частот, МГц	Кількість каналів / частотний план / ширина каналу	Регламентна потужність, Вт	Типовий радіус дії, м
802.15.1 Bluetooth	2400-2483,5	79 (1 МГц)	0,1	10
NFC	13,56	1	0,2	0,1
802.11 WiFi	2400-2483,5	20	0,1	100
802.11b; 802.11g WiFi	2400-2483,5	2412+5(n-1), n = 1, 2 …13	0,1; 0,25	100
802.11a WiFi	5150-5350; 5650-6425	52	0,1; 1	100
802.11n WiFi	2400-2483,5 і / або 5150-5350; 5650-6425	56 (20 МГц), 114 (40 МГц)	0,25; 0,1; 1	100
802.15.4	868,0-868,6; 902-928; 2400-2483,5	1 (Європа); 30 (Америка); 16	0,1	10
Z-Wave	868,4-926,3	Розподіл за регіонами		
LPD 433	433,075-434,775	69	0,1	1000
PMR 446	446-446,1	8 446.00625 + 0.0125 * n, n = 0 ... 7	0,5	1000
GPS L-діапазон	1176.45-1575.42	1176.45 (L5); 1227.60 (L2); 1381.05 (L3); 1575.42 (L1)	~ 50	~ 20* 10^6
ADS-B L-діапазон	962–1213; 978; 1030; 1090	1030 – прийом; 1090 - передавання	75 - 500	30 000

Окрім того, існують технологічні особливості використання радіочастот та відповідних технологій для реалізації типових інфокомунікаційних функцій, як то:

- прийом - передавання даних (наприклад, при голосовому радіообміні, або при моніторингу об’єктів),
- системна радіонавігація (радіомітки, геопозиціювання, тощо),
- дистанційного управління автоматизованими об’єктами (як простих пультів ДУ, так і системних смарт-модулей).

Типовий функціональний розподіл радіочастотних технологій в БСС наведено у табл. 2.

Таблиця 2

Функціональне використання радіочастотних технологій в БСС

	Передавання даних	Приймання даних	Навігація	Управління
Bluetooth	++	++	+	+
NFC	+	+	-	++
WiFi	++	++	+	+
Z-Wave	+	++	-	+
LPD	+	+	-	++
PRM	++	++	-	-
GPS	-	-	++	-
ADS-B	+	+	++	-

(позначення: ++ основне застосування; + можливе застосування; - не застосовується).

Систематизовані таким чином фізичні та функціональні параметри потенційних інфокомунікаційних каналів є першим етапом аналізу радіочастотної кіберуразливості БСС. Такий аналіз є необхідним для оцінювння інфокомунікаційних канали БСС на доступність, автентичність, завадостійкість, а системи в цілому тестувати, зокрема, на радіочастотне проникнення (penetration test, pentesting) та функціональну безпеку (IMECA) [4].

Відмітимо, що запровадження БСС у складі об’єктів критичної інформаційної інфраструктури в Україні чітко регламентовано. Так, на об’єктах критичної інформаційної інфраструктури передача да-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

них безпроводовими мережами повинна здійснюватися виключно захищеними з'єднаннями із забезпеченням її конфіденційності та цілісності [23].

3. Тенденції кіберінцидентів в БСС

Аналіз новітніх тенденцій кіберінцидентів у галузі смарт-систем є важливою складовою побудови системи адекватних заходів кіберзахисту. Так, Агенція Європейської Ради з Кібербезпеки (European Union Agency for Cybersecurity, ENISA) визначає склад інтелектуальних інфраструктур - вони включають низку операторів із різних сфер діяльності, таких як енергетика, громадський транспорт, громадська безпека. Тобто розгортаються і експлуатуються кіберфізичні системи, які являють собою кероване даними обладнання, що взаємодіє з фізичним світом. Ці системи співпрацюють і обмінюються даними за кількома схемами, залежно від рівня їх зрілості. Але використання кіберфізичних пристроїв (пристроїв з програмним керуванням, які взаємодіють з фізичним світом) несе нові ризики і для економіки і для безпеки громадян [24].

Має місце зростаючий темп міграції критично важливих інфраструктур в інтелектуальні інфраструктури шляхом розгортання Інтернету речей, віддаленого управління і аналізу великих даних З одного боку, це поліпшує якість таких сервісів, але зворотною стороною є безпроводова системна архітектура з притаманною радіочастотною кіберуразливістю.

Структуруємо новітні відомі кіберінциденти, щоб визначити узагальнений вектор їх розвитку.

APT атаки

За даними Positive Technologies [25], одного з провідних аналітиків у галузі кібербезпеки, протягом 2019 - 2020 рр. спостерігається загальна тенденція зростання високотехнологічних APT атак (Advanced Persistent Threat, APT – розвинена стійка загроза, також цільова кібератака) з реалізацією на основі високої кваліфікації атакуючих і застосуванні спеціальних технічних засобів та спрямуванням на цільові інформаційно-технологічні інфраструктури. Основні вектори APT нападу – інформаційні, фізичні і обманні.

Основні цілі APT атаки - встановлення несанкціонованої присутності всередині інфраструктури, що атакується для отримання інформації, зриву або створення перешкод її функціонуванню. APT атакам властива адаптація до заходів захисту зі збереженням рівня проникнення в цільову інфраструктуру.

Як наслідок росту високотехнологічних загроз, спостерігається тенденція зміни парадигми кіберзахисту на таку, що здібна викривати (ability to detect) – максимально швидко виявити атаку і атакуючого, щоб мінімізувати зловмисні наслідки та можливості. У зв'язку з цим, зафіксоване трикратне (!) зростання затребуваності високоінтелектуальних засобів захисту: систем класу безпекового менеджменту (security information and event management, SIEM), мережних аналізаторів трафіка (network traffic analysis, NTA) та інших комплексних antiAPT-рішень.

У контексті кібербезпеки важливою є наступна тенденція. У галузі БСС спостерігаються зміщення фокусу послуг: основними споживачами послуг зв'язку поступово стають не люди, а речі. Цьому сприяють вже запущені в ряді країн перші стільникові мережі стандарту 5G, основними споживачами яких стануть пристрої IoT. Захищеність розумних систем на базі IoT-пристроїв безпосередньо залежить від безпеки використовуваних телекомунікаційних технологій. З поширенням мереж 5G і розвитком IoT збільшиться і масштаб загроз: типовими жертвами атак можуть стати підключені автомобілі або системи життєзабезпечення міста, наприклад.

CPS атаки

Кіберфізічна система (Cyber-Physical System, CPS) - це система, яка може ефективно інтегрувати електронні (кібер) і фізичні компоненти, використовуючи сучасні сенсорні, обчислювальні і мережні технології [1, 2]. Нова обчислювальна парадигма, відома як кібер-фізико-соціальні або фізико-кібер-соціальні обчислення [3], виникла з CPS і кіберсоціальних систем (cyber-social systems, CSS). Кібер-фізико-соціальні системи (cyber-physical-social systems, CPSS) розширюють CPS та включають соціальний простір і ознаки участі і взаємодії людей [4]. Повсюдне впровадження CPS пов'язано з концепцією «Індустрія 4.0», яка формує процес об'єднання технологій і знань, забезпечуючи автономність, надійність, системність, контроль без участі людини.

Ключові технологічні тенденції, що лежать в основі CPS, включають: інтернет речей, великі дані, смарт-технології, хмарні обчислення і т.д. CPS системи є основою для розвитку наступних сфер: смарт-виробництво, смарт-медицина, смарт-будівлі та інфраструктури, «розумні» автомобілі, мобільні системи, системи оборони й системи метеоспостережень.

Швидке зростання використання додатків CPS призводить до ряду наступних проблем з інформаційною безпекою та конфіденційністю [27].

Загрози на фізичному / MAC рівні OSI:

- радіоглушіння (Jamming);
- маніпуляції з даними (Tampering with data);
- мережеві колізії (Collision attack);

– відмова у сні (енерговиснаження, Denial-of-sleep, DoSL).

Класифікації загроз CPS включає [27]:

– підміну особистості (Spoofing identity);

– модифікацію даних (Tampering with data);

– відмову від авторства (Repudiation of origin);

– розголошення інформації (Information disclosure);

– підвищення привілеїв (Elevation of privilege);

– відмову в обслуговуванні (Denial of service, DoS).

IoT атаки

До 2025 р. число пристроїв, підключених до Інтернету Речей, згідно з даними [28], досягне 75 мільярдів. Типовими IoT є маршрутизатори, веб-камери, побутова техніка, розумні годинник, медичні прилади, виробниче обладнання, автомобілі та системи безпеки. Підключені пристрої є зручними для споживачів і багато компаній використовують їх щоб заощадити, збираючи в такий спосіб величезні обсяги корисних даних і оптимізуючи бізнес-процеси. Однак, велика кількість підключених пристроїв означає і масштабні кіберуразливості.

За даними агенції Forbes в 2019 р. зростання кібератак на інфраструктуру IoT склало 300% [29].

Як випливає з аналізу [30], основними загрозами для IoT є наступні.

Ботнети. Ботнети (Botnets) поєднують безліч систем для віддаленого контролю над пристроями та системами жертви. Звідси кіберзлочинці можуть збирати конфіденційні дані та здійснювати кібератаки. Пристрої IoT особливо уразливі до цих атак. Наприклад, ботнет Mirai торкнувся 2,5 мільйона пристроїв, включаючи розумні камери, маршрутизатори та принтери. І таке становище це лише погіршується. На основі успіху цих атак кіберзлочинці створюють ще досконаліші бот-мережі IoT.

Атаки "людина посередині". Під час атак "людина посередині" (Man-in-the-middle) хакери перехоплюють комунікації, порушуючи канали зв'язку. Незабаром вони отримують контроль над спілкуванням для надсилання незаконних повідомлень. Оскільки пристрої IoT обмінюються даними в режимі реального часу, атаки "людина посередині" загрожують розумній побутовій техніці, промисловому обладнанню та автономним транспортним засобам. Така уразливість може мати непередбачувані наслідки.

Відмова в обслуговуванні. Атаки відмови в обслуговуванні (DoS) переповнюють системи, надсилаючи багато запитів. DoS атака зазвичай не краде критичних даних, але може вивести з ладу сервіси, завдавши шкоди їхній продуктивності чи репутації. Оскільки пристрої IoT є легкою мішенню, кіберзлочинці також можуть здійснювати атаки і на них. Завантажуючи мережні пристрої фіктивними запитами, вони тимчасово блокують їх штатні функції.

Крадіжка даних. Крадіжка даних (Data Theft) є однією з основних зловмисних цілей атак. Загальновідомі випадки подібних інцидентів, що компрометують дані мільйонів користувачів мереж. Але все частіше кіберзлочинці націлені на пристрої IoT, які, як правило, не мають ніякого захисту. Це можуть бути персональні та медичні засоби IoT (так звані IoMT) - розумні годинники, термостати, кардіопристрої, тощо. Це спричиняє виток як персональної, так і корпоративної інформації.

Скомпрометовані таким чином пристрої можуть стати точкою несанкціонованого входу до корпоративних мереж. У подальшому це може дозволити втручання у бізнес-системи та інші ресурси компанії. Зокрема, розповсюдженим кіберзлочином, що таким чином реалізується є збирання даних про клієнтів або співробітників з метою заподіяти економічну шкоду.

Віддалений запис. Віддалений запис (Remote Recording) це несанкціоноване використання можливостей мережних медіазасобів. У програмному забезпеченні пристроїв IoT можуть бути уразливості, які злочинці використовують для віддаленого скритого запису аудіо- або відеозапису. Хоча ці напади фіксуються рідше, вони також небезпечні. Це становить загрозою витоку конфіденційної інформації. Навіть якщо камера IoT захищена, вона пов’язана з іншими пристроями IoT, можливо з протоколами з нижчим рівнем безпеки. Це дає непряму можливість через мережне втручання отримати доступ до тієї самої камери невдовзі.

Слід підкреслити, що означені IoT атаки можуть бути реалізовані з високою ймовірністю саме через несанкціоноване радіочастотне втручання.

Атаки на мережні інтелектуальні медичні пристрої (IoMT)

Недавній звіт Vectra про IoT у галузі охороні здоров'я [31] вказує на те, що поширення медичних пристроїв Інтернету речей (IoMT) водночас з відсутністю сегментації мереж, недостатнім контролем доступу і залежністю від застарілих систем, привело до збільшення кібератак. Ймовірними цілями таких атак можуть бути:

– особиста інформація пацієнтів;

– конфіденційна медична інформація;

– порушення процесів надання медичних послуг.

Більшість пристроїв IoMT розроблені без урахування вимог кібербезпеки, що робить їх особливо уразливими для злому. Згідно Інституту розробки програмного забезпечення Університету Карнегі-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Меллона: «Чим більше пристроїв підключено до мереж лікарень і клінік, тим більш уразливими будуть ставати дані та інформація про пацієнтів».

Ще більше занепокоєння викликає ризик віддаленої компрометації пристроїв, безпосередньо підключених до пацієнта. Зловмисник теоретично може несанкціоновано збільшити або зменшити лікарські дози, послати сигнали управління на пристрої життєзабезпечення пацієнта або маніпулювати моніторингом показників життєдіяльності.

З іншого боку, оскільки лікарні та медичні установи все ще адаптуються до цифрового оформлення медичних карт пацієнтів, коли медичні записи пацієнтів з конфіденційною медичною інформацією майже повністю онлайн, вони є легкодоступними для хакерів. Ось тільки один приклад. Міністерство внутрішньої безпеки США (US Department of Homeland Security) попередило кардіологів, лікарні і пацієнтів про те, що сотні тисяч імплантованих дефібриляторів і кардіомоніторів можуть бути віддалено скомпрометовані, ряд медичних пристроїв містить уразливості телеметрії, які також можуть призвести до кіберзламування і перехоплення даних. У більшості лікарень є мережі з тисяч підключених пристроїв, які не відслідковуються на предмет аномальної мережної поведінки [32].

Атаки на напівавтономні транспортні засоби і трафік (ATM)

Серійні автівки без водія знаходиться ще в перспективі, але підключені до Інтернету машини - це вже реальність. Підключений автомобіль використовує вбудовані датчики для оптимізації своєї роботи і комфорту пасажирів. Зазвичай це робиться за допомогою вбудованого, прив'язаного або інтегрованого смартфона. Завдяки швидкому розвитку технологій, підключені автомобілі стає все більш поширеними. У 2020 році приблизно 90 відсотків нових автомобілів будуть підключені до Інтернету, про це інформує звіт під назвою «7 тенденцій в області підключених автомобілів, які сприяють майбутньому» [33]. Серед автомобільних технологій, що є вже впровадженими, відзначені такі тренди:

- безпілотні автомобілі;
- інтерфейси штучного інтелекту (AI);
- телематика;
- комунікаційні технології V2V (автомобіль до автомобіля) і V2X (автомобіль до всього);
- датчики, інтегровані з AI;
- бортові мережеві і хмарні сервіси;
- технології B2V (Brain-to-Vehicle).

Навіть якщо автомобіль не є безпілотним, водій пов'язаний з навколишнім світом через цифрову платформу в кабіні, а датчики, розташовані навколо автомобіля, забезпечують безпеку в умовах інтенсивного руху. Перспективні технології «автомобіль-автомобіль» (V2V) і «автомобіль-інфраструктура» (V2I) дозволяють автомобілю обмінюватися даними з іншими автомобілями та інфраструктурою, наприклад, світлофором. Це є основою для запровадження смарт-систем автоматизованого управління трафіком (ATM). Таким чином, наприклад, швидкість автомобіля і безпечну дистанцію до інших автомобілів можна відрегулювати негайно в залежності від дорожніх умов.

Розпізнавання голосу дозволяє водіям спілкуватися з віртуальним персональним помічником (B2V), щоб планувати зустрічі і відправляти текстові повідомлення, не відриваючи рук від керма, в той час як навігаційна система управляє автомобілем.

Для хакерів ця еволюція у виробництві і дизайні автомобілів означає ще одну можливість використовувати уразливості в транспортних смарт-системах. З огляду на ступінь складності та інтегрованості таких систем, найбільш зручною та ймовірною також є саме радіочастотна реалізація атак.

Авіаційна кібербезпека (ACS)

Авіаційна кібербезпека є виключно актуальною проблемою, що відноситься до галузі убезпечення критичних інфрастуктур. Наголосимо, що у технологічному процесі пілотування сучасного повітряного судна (ПС) питома вага автоматизованих систем управління складає 95 відсотків. Серйозною проблемою є потенційна кіберуразливість сучасної авіоніки. Так, відомі численні успішні атаки на безпроводові системи літаків і аеропортів [34].

Реальну загрозу кібербезпеці ПС, зокрема, представляє радіочастотна уразливість широко використовуваної галузевої інформаційної системи ADS-B автоматичного спостереження-радіомовного (Automatic Dependent Surveillance-Broadcast, ADS-B) [35, 36].

За даними Statista, до 2022 року обсяг ринку прикладного ПО для аерокосмічної і оборонної промисловості досягне 3654 $ млн. Кібератаки можуть загрожувати прямо в повітрі найсучаснішим пасажирським і військовим літакам. Обсяг ПО для бортового обладнання повітряного судна в середньому становить кілька мільйонів рядків коду (14 млн – Boeing 787). 95% складових польоту повітряного судна (курс, час руху, маршрут, робота двигунів і т.д.) контролюють в автоматичному режимі.

Використовуючи радіочастотну уразливість безпроводових систем більшості літаків, можливо досить швидко здійснити зловмисне проникнення і навіть керувати літаком ззовні [37].

Наведемо деякі приклади резонансних радіочастотних авіакіберінцидентів:

– 2015 г. – польська авіакомпанія LOT зіткнулася з кібератакою, яка привела до збоїв в наземному обслуговуванні повітряних суден;

– 2016 г. – нелегітимний віддалений доступ до систем управління Boeing 757;

– 2018 г. – злом бортових мереж Wi-Fi, доступ до важливих супутникових і комунікаційних пристроїв в літаку безпосередньо в процесі польоту.

Узагальнюючи, відмітимо наступні актуальні радіочастотні уразливості ПС [38]:

– уразливості бортових мереж передачі даних в комплексі бортового обладнання на основі різних інформаційних протоколів;

– уразливості безпроводових телекомунікаційних та інформаційно-вимірювальних пристроїв на борту ПС;

– уразливості бортових і наземних засобів зв'язку, навігації, спостереження та наведення, що працюють на різних радіочастотах;

– інформаційні атаки зовнішніх зловмисників за безпроводовими каналами передачі даних з ціллю одержати доступ до бортової обчислювальної мережі.

4. Оцінювання радіочастотних уразливостей БСС

Сучасні безпроводові смарт-системи є галуззю, що динамічно розвивається і активно залучає різноманітні радіочастотні інфокомунікаційні технології. Маючі на увазі такі узагальнені параметри можливого несанкціонованого радіочастотного втручання у БСС, як технологічність, вартість, ймовірність, результативність, проведемо якісне (експертне) оцінювання проаналізованих вище технологій (каналів) БСС. У табл. 3 наведені одержані результати у вигляді якісних експертних оцінок потенційних радіочастотних уразливостей інфокомунікаційних каналів БСС за технологіями, що використовуються та в залежності від типів відомих цільових атак.

З огляду на наведені результати слід відмітити особливу небезпеку високотехнологічних APT-атак, а також високу потенційну уразливість БСС як кіберфізичних систем у досліджуваному контексті радіочастотного втручання.

Важливим виявленим у ході роботи трендом є суттєве зниження вартості APT-атак. Це пов'язано з технологічним розвитком програмного радіо [39] (або програмно визначаємого радіо, SDR – Software Defined Radio).

Так, новими можливостями ефективного використання SDR-технологій проникнення є [40]:

– робота у будь-якої частині радіодіапазону;

– перехоплення (запис) радіоповідомлення;

– цифрова обробка (редагування) радіоповідомлення у режимі realtime;

– випромінювання радіоповідомлення за довільним шаблоном.

Таблиця 3

Експертне оцінювання радіочастотних кіберуразливостей БСС у цільових атаках

Канал / тип атаки	APT	CPS	IoT	IoMT	ATM	ACS
802.15.1 Bluetooth	+	+	+	+	+	+
NFC	+	+	+		+	
802.11 WiFi	+	+	+	+	+	+
802.11b; 802.11g WiFi	+	+	+	+	+	+
802.11a WiFi	+	+	+	+	+	+
802.11n WiFi	+	+	+	+	+	+
802.15.4	+	+	+	+	+	+
Z-Wave	+	+	+			
LPD 433	+	+	+		+	
PMR 446	+					
GPS L-диапазон	+				+	+
ADS-B L-диапазон	+					+
Загальна ймовірність радіочастотного втручання, %	100	75	75	50	75	67

Таким чином, застосуванням SDR інфокомунікаційний канал БСС можливо скомпрометувати за такими параметрами, як:

– доступність

– цілісність;

– автентичність;

– конфіденційність;

– своєчасність;

– достовірність.

Керуючись новітньою парадигмою кіберзахисту ability-to-detect та завдяки означеним можливостям SDR, доцільно розробити методики застосування SDR у галузі радіочастотного пентестінгу – як ефективний високотехнологічний інструмент практичного дослідження радіочастотної кіберуразливості безпроводових смарт-систем.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Висновки

У наведеному дослідженні з точки зору потенційної радіочастотної кіберуразливості узагальнено та систематизовано фізичні та функціональні параметри актуальних безпровідних технологій у ISM-діапазоні. Визначено, що означені технології все ширше застосовуються у галузях IoT, IoMT, ATM, Industry 4.0 та інших смарт-системах [41]. Такі рішення ефективно підвищують рівень відповідних сервісів, що надаються. Але пропорційно цьому також вкрай динамічно зростає кількість зафіксованих у цій галузі кіберінцидентів. Тому наслідки можливого несанкціонованого втручання у їх системний інфокомунікаційний радіообмін становить істотну загрозу у галузях інформаційної та функціональної безпеки. Окремо слід зазначити тяжкість наслідків використання означених уразливостей у критичних смарт-інфраструктурах – медичних, транспортних, промислових.

У ході подальших досліджень доцільно виконати детальний теоретичний аналіз можливостей несанкціонованого використання програмно визначаємого радіо та розробити методику SDR-пентестінга БСС.

Підсумовуючи, зазначимо, що слід говорити про застосування SDR у галузі БСС як про новий вектор розвитку їх кібербезпеки, з урахуванням якого можуть бути розроблено нові більш складні і гнучкі сценарії кібератак. Отже, це обумовлює необхідність пошуку та дослідження відповідних засобів кіберзахисту.

Література

1. 802.XX And The IoE [Електронний ресурс]. – Режим доступу: https://semiengineering.com/802-xx-for-the-ioe. – 3.07.2020.

2. Cyber-Physical Systems Security - A Survey [Text] / A. Humayed, J. Lin, F. Li and B. Luo // IEEE Internet of Things Journal. – 2017. - Vol. 4, No. 6. – P. 1802-1831. DOI: 10.1109/JIOT.2017.2703172.

3. Abdulmunem, A. The Method Of IMECA-Based Security Assessment: Case Study For Building Automation System [Text] / Al-Sudani Mustafa Qahtan Abdulmunem, Ahmed Waleed Al-Khafaji, V. S. Kharchenko // Системи обробки інформації. - 2016. - № 1(138). - С. 138-144.

4. Kharchenko, V. Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment [Text] / V. Kharchenko, V. Torianyk // Conference Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2018. – P. 372-377.

5. New Type Of GPS Spoofing Attack In China Creates "Crop Circles" Of False Location Data [Електронний ресурс]. – Режим доступу: https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data . – 3.07.2020.

6. ИКАО - Стратегия в области авиационной безопасности, октябрь 2019 [Електронний ресурс]. – Режим доступу: https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx. – 13.06.2020.

7. EUROCONTROL - Cyber Security in aviation, October 2019 [Електронний ресурс]. – Режим доступу: https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf. - 13.06.2020.

8. Security Requirements Analysis of ADS-B Networks [Електронний ресурс] / T. Kacem, D. Wijesekera, P. Costa, A. Barreto. – Режим доступу: http://ceur-ws.org/Vol-1304/STIDS2014_T06_KacemEtAl.pdf. - 13.06.2020.

9. Sylla, I. The ISM Revolution: The Next Big Thing [Електронний ресурс] / I. T. Sylla. – Режим доступу: https://www.eetimes.com/the-ism-revolution-the-next-big-thing. - 15.06.2020.

10. ISM диапазон [Електронний ресурс]. – Режим доступу: https://ru.qwe.wiki/wiki/ISM_band. – 3.07.2020.

11. Рішення НКРЗІ №18 від 12.01.2012 Про схвалення узагальнених умов застосування радіоелектронних засобів та випромінювальних пристроїв [Електронний ресурс]. - Режим доступу: https://nkrzi.gov.ua/index.php?r=site/index&pg=38&id=805&language=uk. – 3.07.2020.

12. Short range devices [Електронний ресурс]. – Режим доступу: https://www.etsi.org/technologies/short-range-devices?jjj=1598607192016. – 3.07.2020.

13. Bluetooth [Електронний ресурс]. – Режим доступу: - https://www.sciencedirect.com/topics/engineering/bluetooth. – 3.07.2020.

14. Z-Wave [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Z-wave. – 3.07.2020.

15. Near Field Communication Technology Standards [Електронний ресурс]. – Режим доступу: http://nearfieldcommunication.org/technology.html. – 3.07.2020.

16. Торяник, В. Уразливість сучасних технологій радіочастотної ідентифікації [Текст] / В. В. Торяник // Застосування інформаційних технологій у правоохоронній діяльності : Матеріали наук.-практ. семінару. – Харків : ХНУВС, 2015. – С. 66-68.

17. LPD433 [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/LPD433. – 3.07.2020.

18. PMR446 [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/PRM446. – 3.07.2020.

19. L-band [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/L-band. – 3.07.2020.

20. Global Positioning System Standard Positioning Service Performance Standard [Електронний ресурс]. – Режим доступу: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf. - 5.07.2020.

21. Steigenberger, P. GPS and GLONASS Satellite Transmit Power: Update for IGS repro3 [Електронний ресурс] / P. Steigenberger, S. Thoelert, O. Montenbruck. – Режим доступу: https://elib.dlr.de/129734/1/TX_Power_20191021.pdf. – 5.07.2020.

22. Automatic Dependent Surveillance Broadcast (ADS-B) [Електронний ресурс]. – Режим доступу: https://www.skybrary.aero/index.php/Automatic_Dependent_Surveillance_Broadcast_(ADS-B). – 5.07.2020.

23. Постанова КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури») [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#top. – 7.07.2020.

24. IoT and Smart Infrastructures [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure?tab=details. - 8.07.2020.

25. Кибербезопасность 2019-2020. Тренды и прогнозы [Електронний ресурс]. - Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020. – 8.07.2020.

26. Алгулиев, Р. Обеспечение информационной безопасности киберфизических систем [Електронний ресурс] / Р. Алгулиев, Я. Имамердиев, Л. Сухостат. - Режим доступу: https://www.researchgate.net/publication/317634995.-8.07.2020 р. – 8.07.2020. DOI: 10.25045/NCSoftEng.2017.07.

27. Cyber-Physical Attacks are Finally for Real [Електронний ресурс]. – Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/cyber-physical-attacks-are-finally-real. - 8.07.2020.

28. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 [Електронний ресурс]. - Режим доступу: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide. - 8.07.2020.

29. Cyberattacks On IOT Devices Surge 300% In 2019 [Електронний ресурс]. - Режим доступу: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#56aff7955892. – 8.07.2020.

30. Warning: Your IoT devices are at risk of cyber-attack [Електронний ресурс]. - Режим доступу: https://wire19.com/warning-iot-devices-at-risk. – 8.07.2020.

31. The 2020 Spotlight Report on Healthcare [Електронний ресурс]. – Режим доступу: https://www.vectra.ai/resources/2020-spotlight-report-on-healthcare. – 8.07.2020.

32. Strategic Principles for Securing the IoT [Електронний ресурс]. – Режим доступу: https://us-cert.cisa.gov/ncas/current-activity/2016/11/15/Strategic-Principles-Securing-IoT. – 8.07.2020.

33. 7 Connected Car Trends Fueling the Future [Електронний ресурс]. – Режим доступу: https://medium.com/iotforall/7-connected-car-trends-fueling-the-future-946b05325531. – 10.07.2020.

34. Can your flight be hacked? [Електронний ресурс]. - Режим доступу: https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74. – 10.07.2020.

35. Strohmeier, M. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol [Text] / M. Strohmeier, V. Lenders, I. Martinovic. [Електронний ресурс]. – Режим доступу: https://www.cs.ox.ac.uk/files/7239/1307.3664v2.pdf. – 10.07.2020.

36. Kim, Y. ADS-B vulnerabilities and a security solution with a timestamp [Електронний ресурс] / Y. Kim, J. Jo, S. Lee. – Режим доступу: https://www.researchgate.net/publication/321736587. – 10.07.2020.

37. Зегжда, Д. П. Исследование кибербезопасности бортового оборудования воздушного судна [Електронний ресурс] / Д. П. Зегжда. – Режим доступу: http://www.modern-avionics.ru/Files/14-SPbPU-Zegzhda-29.08.2019.pdf. – 10.07.2020.

38. Зыбин, Е. Ю. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна [Електронний ресурс] / Е. Ю. Зыбин. – Режим доступу: https://www.gosniias.ru/pages/d/akb-2018-1-zybin.pdf. – 10.07.2020.

39. Johnson, P. New research LAB leads to unique radio receiver [Text] / P. Johnson // E-Systems Team. - 1985. - Vol. 5, No. 4. - P. 6 – 8.

40. Picod, J.-M. Bringing Software Defined Radio to the Penetration Testing Community [Електронний ресурс] / J.-M. Picod, A. Lebrun, J.-C. Demay. – Режим доступу: http://lib.21h.io/library/N6I45ECV. – 10.07.2020.

41. Dependable IoT for Human and Industry: Modeling, Architecting, Implementation [Text] / V. Kharchenko, A.-L. Kor, A. Rucinski (editors). – River Publishers, Series in Information Science and Technology, Denmark, 2018. – 450 p.

References

1. *802.XX And The IoE*. Available at: https://semiengineering.com/802-xx-for-the-ioe. (accessed 3.07.2020).

2. Humayed A., Lin, J., Li, F. and Luo, B. Cyber-Physical Systems Security – A Survey. *IEEE Internet of Things Journal*, 2017, vol. 4, no. 6, pp. 1802-1831. DOI: 10.1109/JIOT.2017.2703172.

3. Abdulmunem Al-Sudani Mustafa Qahtan, Al-Khafaji Ahmed Waleed, Kharchenko, V. S. The Method Of IMECA-Based Security Assessment: Case Study For Building Automation System. *Systemy obrobky informatsiyi – Systems of information processing*, 2016, vol. 1 (138), pp. 138-144.

4. Kharchenko, V., Torianyk, V. Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment. *Conference Proceedings of*

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018, pp. 372-377. DOI: 10.1109/DESSERT.2018.8409160.

5. *New Type Of GPS Spoofing Attack In China Creates "Crop Circles" Of False Location Data.* Available at: https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data. (accessed 3.07.2020).

6. *IKAO - Strategija v oblasti aviacionnoj bezopasnosti, oktjabr' 2019* [ICAO - Aviation Security Strategy, October 2019]. Available at: https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx. (accessed 13.06.2020).

7. *EUROCONTROL - Cyber Security in aviation, October 2019.* Available at: https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf. (accessed 13.06.2020).

8. Kacem, T., Wijesekera, D., Costa, P., Barreto, A. *Security Requirements Analysis of ADS-B Networks*. Available at: http://ceur-ws.org/Vol-1304/STIDS2014_T06_KacemEtAl.pdf. (accessed 13.06.2020).

9. Sylla, I. T. *The ISM Revolution: The Next Big Thing*. Available at: https://www.eetimes.com/the-ism-revolution-the-next-big-thing. (accessed 13.06.2020).

10. *ISM diapason.* Available at: https://ru.qwe.wiki/wiki/ISM_band. (accessed 3.07.2020).

11. *Rishennya NKRZI #18 vid 12.01.2012 Pro sxvalennya uzagal`neny`x umov zastosuvannya radioelektronny`x zasobiv ta vy`prominyuval`ny`x pry`stroyiv*. [Decision of the NCRCI №18 of 12.01.2012 On approval of generalized conditions for the use of radio-electronic means and radiating devices]. Available at: https://nkrzi.gov.ua/index.php?r=site/index&pg=38&id=805&language=uk. (accessed 3.07.2020).

12. *Short range devices.* Available at: https://www.etsi.org/technologies/short-range-devices?jjj=1598607192016. (accessed 3.07.2020).

13. *Bluetooth.* Available at: https://www.sciencedirect.com/topics/engineering/bluetooth. (accessed 3.07.2020)

14. *Z-Wave.* Available at: https://uk.wikipedia.org/wiki/Z-wave. (accessed 3.07.2020).

15. *Near Field Communication Technology Standards.* http://nearfieldcommunication.org/technology.html. (accessed 3.07.2020).

16. Torianyk, V. V. Urazlyvist' suchasnykh tekhnolohiy radiochastotnoyi identyfikatsiyi [Vulnerability of modern technologies of radio frequency identification]. *Zastosuvannya informatsiynykh tekhnolohiy u pravookhoronniy diyal'nosti. Materialy nauk.-prakt. seminaru.* Kharkiv, KhNUVS Publ., 2015, pp. 66-68. (In Ukrainian).

17. *LPD433.* Available at: https://uk.wikipedia.org/wiki/LPD433. (accessed 3.07.2020).

18. *PRM446.* Available at: https://uk.wikipedia.org/wiki/PRM446. (accessed 3.07.2020).

19. *L-band.* Available at: https://en.wikipedia.org/wiki/L-band. (accessed 3.07.2020).

20. *Global Positioning System Standard Positioning Service Performance Standard.* Available at: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf. (accessed 5.07.2020).

21. Steigenberger, P., Thoelert, S., Montenbruck, O. *GPS and GLONASS Satellite Transmit Power: Update for IGS repro3*. Available at: https://elib.dlr.de/129734/1/TX_Power_20191021.pdf. (accessed 5.07.2020).

22. *Automatic Dependent Surveillance Broadcast (ADS-B).* Available at: https://www.skybrary.aero/index.php/Automatic_Dependent_Surveillance_Broadcast_(ADS-B). (accessed 5.07.2020).

23. Postanova KMU vid 19 chervnya 2019 r. # 518 *«Pro zatverdzhennya Zahal'nykh vymoh do kiberzakhystu ob"yektiv krytychnoyi infrastruktury»* [Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019 № 518 "On approval of the General requirements for cyber-protection of critical infrastructure"]. Available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#top. (accessed 7.07.2020).

24. *IoT and Smart Infrastructures*. Available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure?tab=details. (accessed 8.07.2020).

25. *Kiberbezopasnost' 2019-2020. Trendy i prognozy* [Cybersecurity 2019-2020. Trends and forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020. (accessed 8.07.2020).

26. Alguliev, R., Imamerdiev, Ja., Suhostat, L. *Obespechenie informacionnoj bezopasnosti kiberfizicheskih system* [Ensuring of information security of cyber-physical systems]. Available at: https://www.researchgate.net/publication/317634995. (accessed 8.07.2020). DOI: 10.25045/NCSoftEng.2017.07.

27. *Cyber-Physical Attacks are Finally for Real*. Available at: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/cyber-physical-attacks-are-finally-real. (accessed 8.07.2020).

28. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide. (accessed 8.07.2020).

29. *Cyberattacks On IOT Devices Surge 300% In 2019.* Available at: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#56aff7955892. (accessed 8.07.2020).

30. *Warning: Your IoT devices are at risk of cyber-attack.* Available at: https://wire19.com/warning-iot-devices-at-risk. (accessed 8.07.2020).

31. *The 2020 Spotlight Report on Healthcare*. Available at: https://www.vectra.ai/resources/2020-spotlight-report-on-healthcare. (accessed 8.07.2020).

32. *Strategic Principles for Securing the IoT.* Available at: https://us-cert.cisa.gov/ncas/current-activity/2016/11/15/Strategic-Principles-Securing-IoT. (accessed 8.07.2020).

33. *7 Connected Car Trends Fueling the Future.* Available at: https://medium.com/iotforall/7-connected-

car-trends-fueling-the-future-946b05325531. (accessed 10.07.2020).

34. *Can your flight be hacked?* Available at: https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74. (accessed 10.07.2020).

35. Strohmeier, M., Lenders, V., Martinovic, I. *On the Security of the Automatic Dependent Surveillance-Broadcast Protocol.* Available at: https://www.cs.ox.ac.uk/files/7239/1307.3664v2.pdf. (accessed 10.07.2020).

36. Kim, Y., Jo, Ju-Y., Lee, S. *ADS-B vulnerabilities and a security solution with a timestamp*. Available at: https://www.researchgate.net/publication/321736587. (accessed 10.07.2020).

37. Zegzhda, D. P. *Issledovanie kiberbezopasnosti bortovogo oborudovanija vozdushnogo sudna* [Study of the cybersecurity of aircraft on-board equipment]. Available at: *http://www.modern-avionics.ru/Files/14-SPbPU-Zegzhda-29.08.2019.pdf.* (accessed 10.07.2020).

38. Zybin, E. Ju. *Koncepcija obespechenija informacionnoj bezopasnosti bortovogo oborudovanija vozdushnogo sudna* [The concept of ensuring of information security of aircraft onboard equipment]. Available at: https://www.gosniias.ru/pages/d/akb-2018-1-zybin.pdf. (accessed 10.07.2020).

39. Johnson, P. New research LAB leads to unique radio receiver. *E-Systems Team*, 1985, vol. 5, no. 4, pp. 6-8.

40. Picod, J.-M., Lebrun, A., Demay, J.-C. *Bringing Software Defined Radio to the Penetration Testing Community*. Available at: http://lib.21h.io/library/N6I45ECV. (accessed 10.07.2020).

41. Kharchenko, V., Kor, A.-L., Rucinski, A. (editors). *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation.* River Publishers, Series in Information Science and Technology, Denmark. 2018. 450 p.

Надійшла до редакції 15.08.2020, розглянута на редколегії 16.11.2020

КИБЕРБЕЗОПАСНОСТЬ БЕЗПРОВОДНЫХ СМАРТ-СИСТЕМ: КАНАЛЫ ВТОРЖЕНИЙ И РАДИОЧАСТОТНЫЕ УЯЗВИМОСТИ

В. Я. Певнев, В. В. Торяник, В. С. Харченко

Предметом данного исследования является радиочастотная киберуязвимость технологии информационно-управляющего взаимодействия в беспроводных смарт-системах (БСС). БСС - это киберфизические системы, работающие в рамках модели OSI. Специфика и специализация таких систем определяется радиотехнологиями физического уровня, так, например, видами БСС являются Интернет Вещей (IoT, том числе медицинский IoMT), Интернет Дронов (IoD), системы авиамониторинга ADS-B и управления траффиком АТМ, а в перспективе - системы Интернета Всего (IoE). **Целью** является анализ радиочастотных параметров информационно-управляющего взаимодействия в БСС для выявление возможных радиочастотных киберуязвимостей БСС. **Задачи**: обобщить и систематизировать физические и функциональные параметры беспроводных технологий в диапазонах ISM (Industrial Scientific & Medical Band) и SRD (Short range devices) существенные с точки зрения радиочастотной киберуязвимости БСС, включая также навигационные технологии. Проанализировать тренды и методы успешных кибератак на БСС. Выполнить экспертные оценки потенциальной киберуязвимости БСС в зависимости от их архитектуры и области применения. Используемыми **методами** являются: анализ трендов известных радиочастотных инцидентов и экспертные оценки киберуязвимости информационно-управляющих каналов БСС. Получены следующие **результаты**. Проанализированы 12 актуальных радиотехнологий БСС. Типизированы 6 видов возможных радиочастотных кибератак на БСС. Выполнено экспертное оценивание вероятности использования уязвимостей по диапазонам, радиотехологиям и видам атак. Показана особая опасность высокотехнологических целевых APT-атак, а также высокая потенциальная радиоуязвимость БСС как киберфизических систем. Особо отмечена киберуязвимость авиационных систем ADS-B. **Выводы**. Научная новизна полученных результатов заключается в следующем: выявлены тренд снижения стоимости APT-атак и рост вероятности их реализации с помощью новых возможностей SDR-технологии (Software Defined Radio – программно определяемое радио). Показана возможность управляемой SDR-компрометации параметров безопасности каналов БСС в любом радиодиапазоне. Предложено перспективное направление исследований – SDR-пентестинг БСС.

Ключевые слова: беспроводная смарт-система; радиочастотное информационно-управляющее взаимодействие; радиочастотная киберуязвимость; авиакибербезопасность; программно-определяемое радио; SDR-пентестинг.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

CYBER SECURITY OF WIRELESS SMART SYSTEMS: CHANNELS OF INTRUSIONS AND RADIO FREQUENCY VULNERABILITIES

V. Pevnev, V. Torianyk, V. Kharchenko

The subject of this study is the radio frequency cyber vulnerability of information and control interaction technology in the wireless smart systems (WSS). WSS is the cyber-physical systems, that operate within the OSI model. The specificity and specialization of these systems are determined by radio technologies of the physical layer. For example, the Internet of Things (IoT, including medical IoMT), the Internet of Drones (IoD), systems for aviation monitoring ADS-B and traffic management ATM, and, in the future, the Internet of Everything (IoE) - all are types of WSS. **The aim** is to analyze the radio frequency parameters of information and control interaction in the WSS to identify possible radio frequency cyber vulnerabilities in the WSS. **Objectives**: summarize and systematize the physical and functional parameters of wireless technologies in the ISM (Industrial Scientific & Medical Band) and SRD (Short range devices) ranges, which are significant from the WSS radiofrequency cyber vulnerability perspective, including navigation technologies; analyze trends and methods of successful cyber attacks on the WSS; carry out expert assessments of potential WSSs cyber vulnerabilities depending on their architecture and application area. **The methods** used: analysis of trends in known radiofrequency incidents and expert assessments of the cyber vulnerability of the WSS information and control interaction channels. The following **results** were obtained: 12 actual WSS radio technologies were analyzed. 6 types of possible radio frequency cyber attacks on the WSS were typified. The expert assessment of the probability of exploiting vulnerabilities by ranges, radio technologies, and attack type was made. The special danger of high-tech targeted APT attacks, as well as the high potential radio vulnerability of cyber-physical systems, was shown. The cyber vulnerability of ADS-B aircraft systems was especially noted. **Conclusions**. The scientific novelty of the results obtained is as follows: a trend of APT attacks cost reduction and an increase in the probability of their implementation through the new capabilities of SDR technology (Software Defined Radio) were revealed. The possibility of a controlled SDR compromising of the security parameters of WSS channels in any radio range was shown. A promising direction of research was proposed - SDR-penetration testing of WSS.

Keywords: wireless smart system; radio frequency information and control interaction; radio frequency cyber vulnerability; aviation cyber security; software-defined radio; SDR-pentesting.

Певнев Володимир Якович – канд. техн. наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Торяник Володимир Володимирович – канд. фіз. -мат. наук, доцент, Харків, Україна.

Харченко Вячеслав Сергійович – Лауреат Державної премії України, заслужений винахідник України, д-р техн. наук, професор, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Vladimir Pevnev – PhD, Assistant Professor of the Department of Computer systems, networks and cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.pevnev@csn.khai.edu, ORCID: 0000-0002-3949-3514, Scopus Author ID: 57194525720, ResearcherID:

Volodymyr Torianyk – PhD, Assistant Professor, Kharkiv, Ukraine,
e-mail: v.toryanyk@khai.edu, ORCID: 0000-0001-7902-8812.

Vyacheslav Kharchenko – Honored inventor of Ukraine, Doctor of Science on Engineering, Professor, Head of the Department of Computer systems, networks and cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: V.Kharchenko@csn.khai.edu, ORCIDID: 0000-0001-5352-077X, Scopus Author ID: 22034616000, ResearcherID: A-7719-2017.