Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.044

УДК 004: 054

МЕТОДОЛОГІЯ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ ТА ІНТЕРНЕТУ РЕЧЕЙ В ІНТЕЛЕКТУАЛІЗАЦІЇ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

В. Б. Дудикевич, Г. В. Микитин, Л. Л. Бортнік, Т. Р. Стосик

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: vdudykev@gmail.com, cosmos-zirka@ukr.net, leonid.l.bortnik@lpnu.ua, taras.r.stosyk@lpnu.ua

Запропоновано багаторівневу структуру безпечної інтелектуалізації інфраструктури суспільства "об'єкти – кіберфізичні системи" у функціональному просторі "відбір – обмін інформацією – оброблення – управління" за профілями – конфіденційність, цілісність, доступність для "розумного екологічного моніторингу", "розумної освіти", "розумної енергетики", "розумної транспортної системи" та інших предметних сфер.

Багаторівнева структура "об'єкти – кіберфізичні системи" безпечної інтелектуалізації розкривається парадигмою "багаторівнева кіберфізична система – багаторівнева інформаційна безпека", яка є підґрунтям для побудови комплексних систем безпеки технологій фізичного простору, комунікаційного середовища, кібернетичного простору.

Побудовано ієрархічну модель безпеки інтернету речей на основі трирівневої архітектури і концепції "об'єкт – загроза – захист". Проаналізовано комплексну модель безпеки безпровідного комунікаційного середовища кіберфізичних систем для сегментів інтелектуалізації інфраструктури суспільства. Представлена методологія безпечних процесів інтелектуалізації дає змогу реалізувати комплексні системи безпеки технологій функціонування об'єктів інфраструктури суспільства.

Ключові слова: інтелектуалізація, інформаційна безпека, об'єкти, кіберфізична система, багаторівнева структура, парадигма безпеки, інтернет речей, ієрархічна модель, комплексна модель.

Вступ

Постановка проблеми. Сьогодні розгортаються процеси інтелектуалізації у просторі Української стратегії індустрії 4.0, які передбачають: впровадження інтелектуальних технологій в різних сегментах інфраструктури суспільства як інструментарію функціонування інтелектуальних об'єктів; розвиток методологій безпеки [1, 2]. Кіберфізичні системи (КФС) та інтернет речей у їх складі, як основні технології четвертої промислової революції, забезпечують життєвий цикл інформації в автоматизованих процесах функціонування промислових об'єктів від відбору та обміну, аналізу та оброблення до інтелектуальної підтримки прийняття рішення на управління станом об'єкта інфраструктури [3].

1. Огляд літературних джерел

Науковці аналізують підходи до забезпечення безпеки кіберфізичних систем, зокрема, як технологій функціонування об'єктів інфраструктури суспільства, зокрема критичної [4, 5, 6, 7]. Ефективність процесів інтелектуалізації інфраструктури суспільства визначається функціонуван-

ням інтернету речей трирівневої архітектури [8], для кожного з рівнів якого характерний різний комплекс загроз [9, 10]. Функціональність рівня сприйняття підтримується комплексом пристроїв, давачів, що здійснюють відбирання інформації від об'єктів фізичного простору. Наприклад, мікроелектромеханічні системи-давачі – 2JCIE-BL, BPS240, BME680, використовуються для відбирання інформації від фізичних об'єктів в інтелектуальних технологіях екологічного моніторингу параметрів компонент довкілля. Транспортний – здійснює передавання інформації для подальшого її оброблення. Прикладний – реалізує оброблення даних та взаємодію із користувачем. Безпеці безпровідних технологій зв'язку, зокрема сенсорних мереж, присвячено багато наукових публікацій, зокрема в роботах [11, 12] висвітлено: аспекти захисту інформації в безпровідних технологіях GSM, CDMA, WiMAX, LTE, Zigbee, Wi-Fi, Bluetooth згідно з концепцією "об'єкт – загроза – захист" та моделлю OSI; особливості безпеки КФС "Wi-Fi – Bluetooth – хмарні обчислення – IoT"; специфіку КСБ кіберфізичної системи на "iPhone – Wi-Fi, Bluetooth – давачі". В закордонних працях [13, 14, 15, 16] розвинуто сучасні тенденції захисту інформації в безпровідних технологіях, зокрема, архітектура, протоколи, загрози, підходи до розв'язання проблеми безпеки, серед яких – елементи прикладної криптографії. Розвиток підходів до безпеки технологій інтелектуалізації на основі структури "об'єкти – кіберфізичні системи – загрози – захист" надасть безпечне функціонування об'єктів інфраструктури суспільства у просторі "відбір інформації – обмін – оброблення – управління".

2. Постановка завдання

Поставка завдання: 1) запропонувати ідеологію безпеки кіберфізичних систем та інтернету речей на рівні багаторівневої структури безпечної інтелектуалізації об'єктів; 2) розробити нову модель комплексної системи безпеки КФС на рівні парадигми "багаторівнева система – багаторівнева безпека"; 3) створити модель безпеки трирівневої архітектури інтернету речей та розвинути модель безпеки безпровідних технологій зв'язку у просторі "загрози – технології захисту". *Мета роботи* – створення методології безпечної інтелектуалізації об'єктів інфраструктури суспільства, яка надаватиме безпечний життєвий цикл інформації у просторі "відбір – обмін інформацією – оброблення – управління" на основі функціонування багаторівневих моделей безпеки КФС, інтернету речей, безпровідних мереж.

3. Багаторівнева структура безпечної інтелектуалізації об'єктів інфраструктури на основі кіберфізичних систем

Вектори програми "Горизонт – Європа" та основні напрями розвитку України у просторі Національної стратегії Індустрії 4.0 дають змогу виділити сегменти впровадження інтелектуальних технологій – екологічний моніторинг компонент довкілля, освіту, енергетичні системи, транспортні системи, які взаємодіють між собою та системно формують "розумну інфраструктуру" країни з такими характеристиками, як: інтероперабельність; віртуалізація; децентралізація; реальний час; орієнтація на сервіси, модульність. В контексті "розумної екології" актуальним аспектом є система локального і глобального динамічного екологічного моніторингу параметрів довкілля, зокрема дослідницький екологічний моніторинг "програма – ІТ – методологія оцінювання якості води", який запроваджують у разі виникнення аварійного забруднення, коли контрольний і робочий моніторинг не задовольняють потреби екологічних цілей, спрямованих на нормалізацію стану компонент довкілля.

Для моніторингу стану якості компонент довкілля, наприклад водних об'єктів, впроваджені інтелектуальні системи вимірювання їх параметрів, серед яких – інтелектуальні геоінформаційні системи та дистанційне зондування Землі з використанням супутника Landsat-8 для отримання мультиспектральних знімків поверхневого шару води у тепловому інфрачервоному каналі і, на цій основі, визначення її температури як одного з основних показників якості [17]. Для моніторингу комплексних показників води, ґрунту, повітря ефективно використовують високомобільні лабораторії

екологічного моніторингу, основними складниками яких є: інтелектуальна інформаційна вимірювальна система; комплекс автономних вимірювальних пристроїв для вимірювання специфічних параметрів довкілля; засоби відбору проб води, ґрунту, повітря; вимірювальний дрон; технічні засоби системи позиціонування GPS; технічні засоби системи безпровідного зв'язку GSM; система управління функціонуванням лабораторії [18]. Національна програма інформатизації в Україні спрямовує розвиток центрів інформаційного забезпечення закладів вищої освіти і впровадження безпечних інформаційно-комунікаційних технологій, серед яких: сервери, персональні комп'ютери, вебсайти, віртуальні навчальні середовища, електронні архіви, безпровідні технології зв'язку.

Концепція цифрової трансформації освіти і науки в Україні передбачає врахування зарубіжного досвіду і реалізацію через напрями: 1) ефективного використання цифрових технологій в освітньому процесі; оптимізації процесів управління, регулювання та моніторингу, які цілісно передбачають створення цифрового освітнього середовища, оснащеного комп'ютерним і мультимедійним обладнанням, сучасними комунікаційними технологіями; 2) підвищення кваліфікації науково-педагогічних працівників закладів освіти у контексті цифрових компетентностей; розроблення системи стандартів у сфері цифрових технологій і стандартів вищої освіти, які гармонізовані з міжнародними стандартами ISO. "Розумні енергосистеми" і "розумні транспортні системи" сьогодні є дуже актуальними сегментами інтелектуалізації промислової інфраструктури країни, які передбачають впровадження безпечних інтелектуальних кіберфізичних систем та застосування криптографічних засобів забезпечення захищеного обміну інформації в безпровідних технологіях зв'язку, зокрема, ефективних алгоритмів шифрування для забезпечення безпеки інформаційних ресурсів користувачів.

Розглянемо багаторівневу структуру безпечної інтелектуалізації інфраструктури (БІІ) суспільства, яка створена на основі КФС та концепції "об'єкт – загроза – захист" (рис. 1).

Рис. 1. Багаторівнева структура безпечної інтелектуалізації об'єктів інфраструктури на основі КФС

Перший рівень – функціональний, що забезпечує працездатність системи "розумні об'єкти" ($О_{1\text{-}N(R,S,T)}$) – кіберфізичні системи ($КФС_{1\text{-}N(R,S,T)}$)" відповідно до інфраструктури: N – "розумна екологія" (РЕк), R – "розумна освіта" (РО), S – "розумна енергетика" (РЕн), T – "розумна транспортна система" (РТС). Другий – інтеграції рівнів КФС "інтернет речей ($IP_{1\text{-}N(R,S,T)}$) – безпровідні технології ($БТ_{1\text{-}N(R,S,T)}$) – комп'ютерні системи ($КС_{1\text{-}N(R,S,T)}$)" та інтеграції компонент одного рівня. Третій рівень – процеси "відбору інформації ($В_{1\text{-}N(R,S,T)}$) / контролю – передавання / приймання ($ПРД_{1\text{-}N(R,S,T)}$/$ПРМ_{1\text{-}N(R,S,T}$) – оброблення інформації ($О_{1\text{-}N(R,S,T)}$) / управління ($У_{1\text{-}N(R,S,T)}$)". Четвертий рівень – загрози безпеці рівням функціональності КФС ($a_{1\text{-}N}$ – $b_{1\text{-}N}$ – $c_{1\text{-}N}$ (РЕк); $d_{1\text{-}R}$ – $e_{1\text{-}R}$ – $f_{1\text{-}R}$ (РО); $g_{1\text{-}S}$ – $h_{1\text{-}S}$ – $i_{1\text{-}S}$ (РЕн); $k_{1\text{-}T}$ – $l_{1\text{-}T}$ – $m_{1\text{-}T}$ (РТС). П'ятий рівень – технології безпеки апаратного і програмного рівнів за основними профілями ($A_{1\text{-}N}$ –$B_{1\text{-}N}$ – $C_{1\text{-}N}$ (РЕн); $D_{1\text{-}R}$ – $E_{1\text{-}R}$ – $F_{1\text{-}R}$ (РО);$G_{1\text{-}S}$ – $H_{1\text{-}S}$ – $I_{1\text{-}S}$ (РЕн); $K_{1\text{-}T}$ – $L_{1\text{-}T}$ – $M_{1\text{-}T}$ (РТС).

4. Парадигма "багаторівнева структура КФС – багаторівнева інформаційна безпека"

Розглянемо парадигму "багаторівнева структура КФС – багаторівнева інформаційна безпека" (рис. 2). Багаторівнева ієрархічна структура КФС: фізичний простір (ФП) – інтернет речей, що взаємодіє з фізичними об'єктами/ пристроями, в які вбудовані давачі; комунікаційне середовище (КС) – безпровідні технології зв'язку, хмарні технології, провідні технології; кібернетичний простір (КП) – інформаційні системи, інформаційні ресурси, інформаційні процеси.

Багаторівнева структура КФС функціонує на рівні двох каналів – вимірювального та управління. Мережа давачів на основі МЕМС-технологій, які поєднують мікроелектронні та мікромеханічні системи, а також виконавчих пристроїв у процесі моніторингу об'єктів інфраструктури формують інформацію відбору (вимірювання, реєстрації) про стан їх параметрів, яка передається з фізичного простору КФС безпровідними мережами в кібернетичний простір для зберігання, оброблення, аналізу й ухвалення управлінського рішення. У кібернетичному просторі КФС на основі аналізу обробленої інформації, порівняння з нормованими параметрами функціонування відповідного об'єкта і виявлення відхилення їх від норми комп'ютерна система приймає рішення щодо управління станом об'єкта через комунікаційне середовище та фізичний простір КФС.

Парадигма "багаторівнева структура КФС – багаторівнева інформаційна безпека" побудована на основі системного підходу, який полягає у застосуванні принципів ієрархічності, структуризації, цілісності, що дають підстави для створення комплексної системи безпеки кіберфізичних систем у сегменті оптимального поєднання: нормативно-правового, організаційного, інформаційного, технічного (апаратного), програмного забезпечення на етапах безпечного життєвого циклу інформації.

Парадигма зумовлюється структурою: класифікація загроз – формування критеріїв захищеності – створення моделі багаторівневої КСБ КФС – вибір методу оцінювання стану захищеності кіберфізичної системи. Основою побудови багаторівневої КСБ КФС є: універсальна платформа "загрози – профілі – інструментарій"; модель системи безпеки ФП, КС, КП; нормативний документ НД ТЗІ 3.7-001-99, що регламентує: вимоги до КСБ у частині захисту від несанкціонованого доступу; вимоги до КСБ у частині захисту від витоку інформації технічними каналами.

Комплексна система безпеки ФП, що пов'язаний з інтернетом речей і залучає: фізичні пристрої, в які вбудовані давачі, зокрема, мікроелектромеханічні системи-давачі (IEEE 2700-2014), виконавчі пристрої, які вбудовані у фізичні об'єкти, створюється згідно з концепцією "об'єкт – загроза – захист".

Комплексна система безпеки КС, що охоплює: безпровідні технології (ДСТУ ISO/IEC 7498); хмарні технології (ДСТУ ISO/IEC 17788:2017, NIST); провідні технології зв'язку (мережі на основі коаксіального (ДСТУ EN 50117) та волоконно-оптичного кабелів (ДСТУ IEC 60794), створюється згідно з концепцією "об'єкт – загроза – захист".

Комплексна система безпеки КП, що охоплює інформаційні ресурси – випадкові, цілеспрямовані загрози – апаратно-програмний захист; інформаційні системи – випадкові, цілеспрямовані

загрози – апаратно-програмний багаторівневий захист; інформаційні процеси – випадкові, цілеспрямовані загрози – апаратний, програмний захист (ДСТУ ISO/IEC 15408), формується згідно з концепцією "об'єкт – загроза – захист".

Управління ІБ багаторівневої кіберфізичної системи ґрунтується на методології застосування методів, зокрема, базового (ISO/IEC TR 13335-3:2007) і моделей управління ІБ, зокрема, моделі "плануй – виконуй – перевіряй – дій" (ISO/IEC 27001:2010) для коригування структури комплексної системи безпеки і забезпечення ефективності захисту інформації.

Парадигма "багаторівнева структура КФС – багаторівнева інформаційна безпека" є універсальною у просторі функціональних задач безпечної інтелектуалізації об'єктів інфраструктури – моніторингу, прогнозування, діагностики, інтерпретації, ідентифікації та ін., зокрема із залученням у кібернетичній структурі технологій штучного інтелекту таких, як експертні системи і нейромережі.

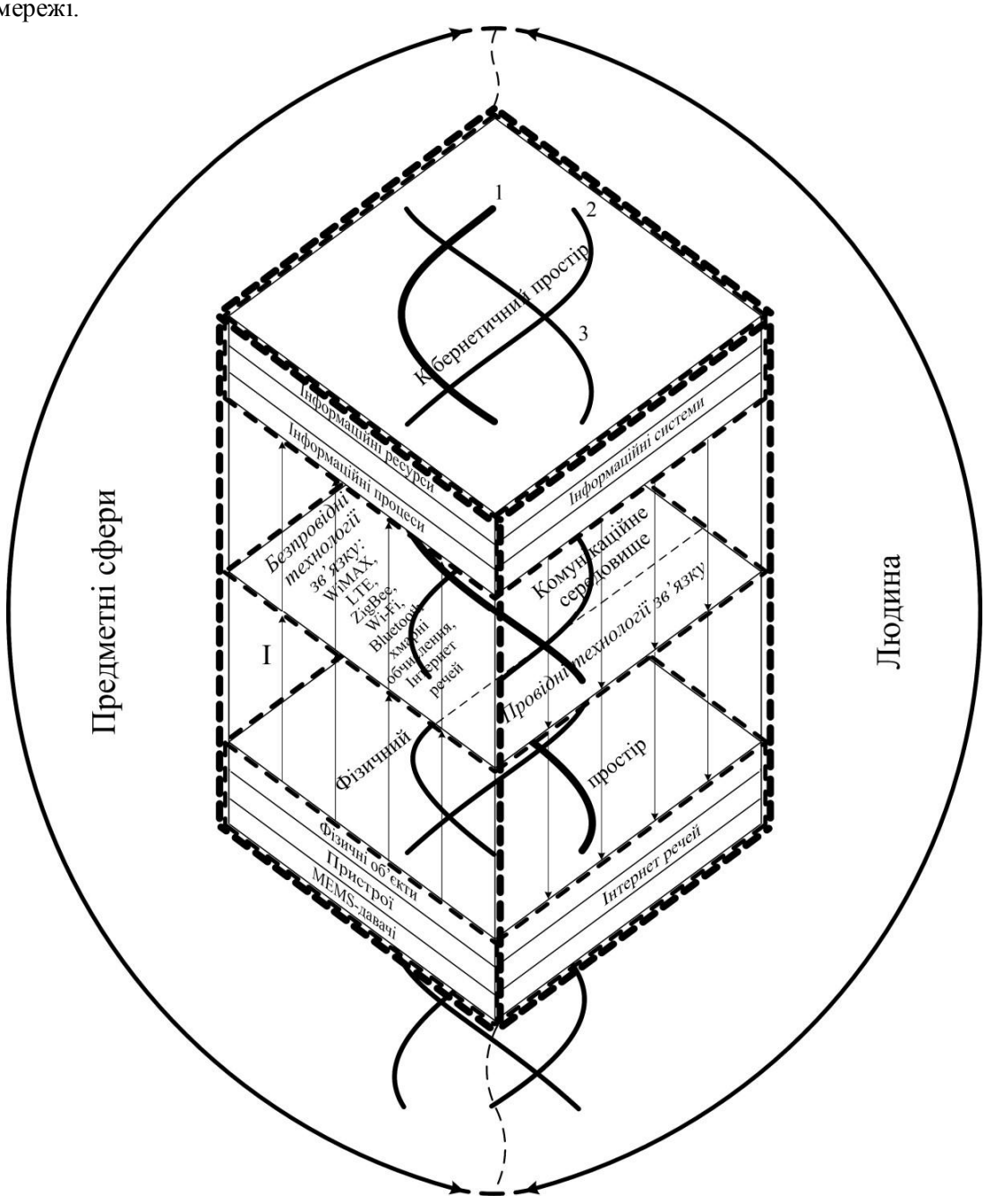

Рис. 2. Структура парадигми побудови КСБ кіберфізичних систем

5. Ієрархічна модель безпеки трирівневої архітектури інтернету речей

Одним з підходів до безпечного функціонування інтернету речей є створення ієрархічної моделі на основі концепції "об'єкт – загроза – захист" та системних принципів – цілісності, ієрархічності та структуризації.

Структура ієрархічної моделі безпеки інтернету речей (рис. 3) має такі особливості: 1) на кожному рівні архітектури інтернету речей подано види загроз, які розгорнуто їх підвидами; 2) відповідно до рівнів сприйняття, транспортного, прикладного – представлено види технологій безпеки, які розгорнуто їх різновидом. За цією структурою наведемо приклади для кожного рівня інтернету речей: однієї загрози та прояву її підвидів; однієї технології безпеки, розгорнувши її функціональну реалізацію різновидами засобів.

Рівень сприйняття. Для цього рівня характерна найбільша кількість загроз основним профілям безпеки (ДСТУ ISO/IEC 15408), оскільки він піддається впливу комплексу загроз, пов'язаних із функціональною безпекою пристроїв і давачів, що взаємодіють з фізичними об'єктами. Загроза – атаки на вузли (давачі та інші пристрої, що взаємодіють із фізичним середовищем). Підвиди – знищення вузла (пошкодження пристрою аж до повного виведення його із ладу з метою порушення роботи системи та переривання процесу збирання інформації), викрадення (зазвичай здійснюється для отримання доступу до чутливої інформації, що може зберігатися на пристрої), підміна (заміна оригінального пристрою на сторонній, запрограмований зловмисником та призначений для несанкціонованого доступу до мережі і передавання фальшивих даних) і глушіння вузла (генерування завад задля унеможливлення передавання інформації від вузла до мережі). На цьому рівні основним методом захисту інформації є забезпечення фізичної безпеки вузлів, що досягається через розміщення відповідних пристроїв у межах контрольованої зони.

Транспортний рівень. Загроза – мережеве прослуховування (перехоплення комунікацій між пристроями в мережі). Підвиди – пасивне (без прямого втручання і зміни інформації), активне (атака "людина посередині", редагування інформації, що передається), аналіз трафіку (прослуховування мережевих комунікацій без компрометації даних, для визначення місць розташування вузлів, структури маршрутизації). Важливою технологією безпеки є застосування систем виявлення вторгнень (IDS), які можуть бути представлені мережевими (NIDS), хостовими (HIDS) та навіть системами запобігання вторгненням (IPS).

Прикладний рівень. Загроза – шкідливі програми. Підвиди – поширені в інтернеті речей програми-вимагачі, шпигунські програми, трояни та хробаки. Одним із методів захисту цього рівня є організація розроблення безпечного програмного забезпечення, що реалізується за трьома технологіями: методикою безпечного кодування, статичним і динамічним аналізом коду та детальною перевіркою помилок усього внутрішньо розробленого програмного забезпечення. Ієрархічна модель безпеки інтернету речей уможливить побудову комплексної системи безпеки трирівневої архітектури на основі критеріїв вибору: моделі загроз, моделі порушника, моделі безпеки.

Критерієм вибору загроз ІБ трирівневої архітектури інтернету речей, представлених в системній моделі, є ступінь порушення функціональної безпеки об'єктів (систем) інфраструктури, що унеможливлює забезпечення їх гарантоздатності і викликає функціонування систем у просторі їх інформаційно-технічних станів: частково працездатний (безпечний), непрацездатний (безпечний), непрацездатний (небезпечний) (СОУ-Н НКАУ 0060:2010). Критерієм вибору технологій безпеки є оптимальна ефективність протидії комплексу загроз та їх підвидам на одному з рівнів інтернету речей.

Ієрархічна модель безпеки інтернету речей є підгрунтям для формування комплексної системи безпеки, яка трансформується в різновиди залежно від об'єкта інфраструктури, комплексу загроз, технологій захисту інформації.

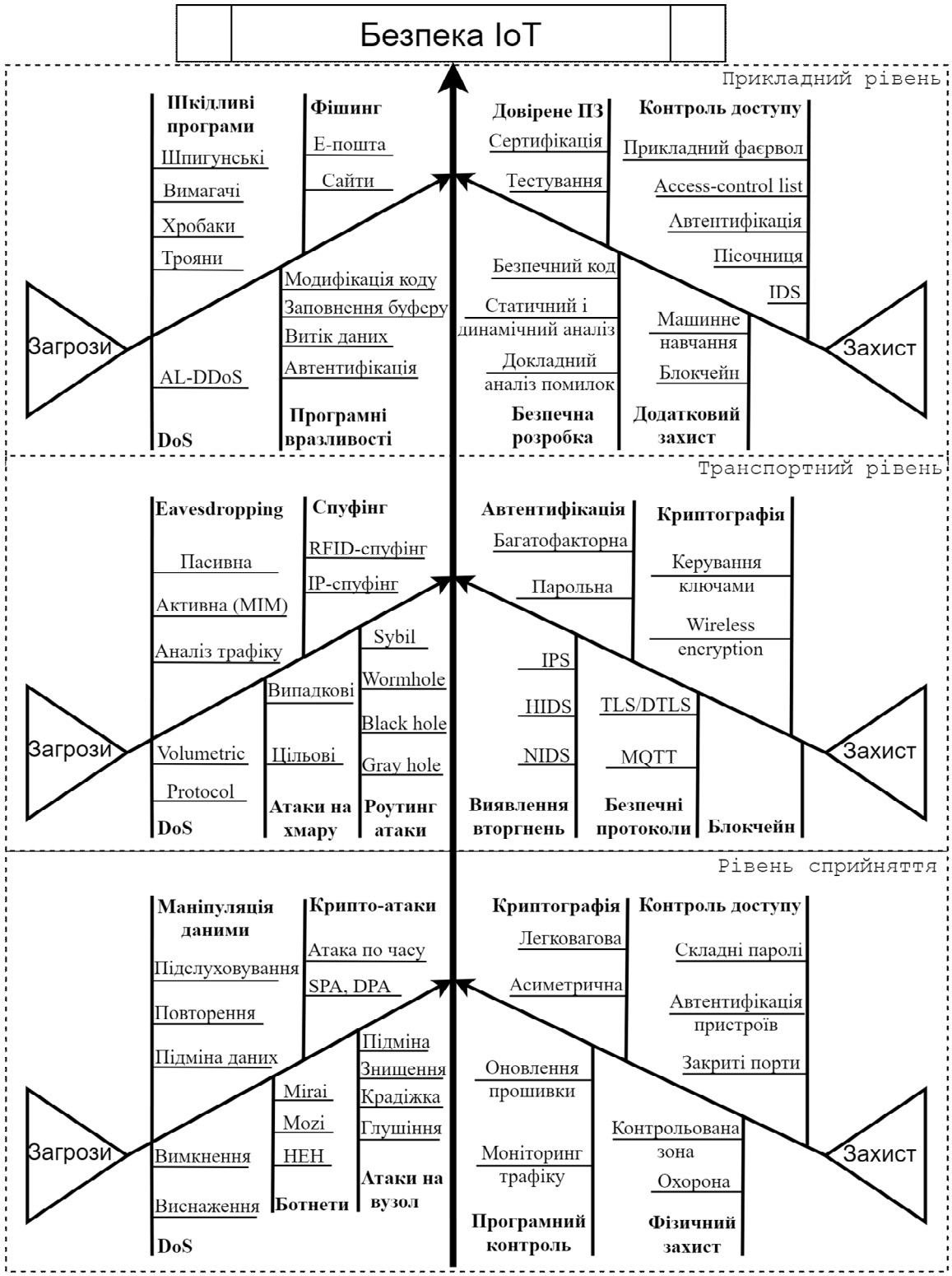

Рис. 3. Ієрархічна модель безпеки трирівневої архітектури інтернету речей

6. Комплексна модель безпеки безпровідних технологій зв'язку

У контексті розвитку технологій ІБ безпровідних сенсорних мереж актуальними є: 1) методи моделювання функціонування сенсорних мереж, зокрема параметрів сигналів інформаційних вузлів як складових частин мереж, у режимах протидії атакам; 2) дослідження уразливостей сенсорних

підмереж архітектури інтернету речей за умов впливу комплексу атак [19]. Сучасні тенденції безпеки безпровідних сенсорних мереж розвинуто у підходах, що ґрунтуються, зокрема, на застосуванні криптосистеми RSA для захищеного обміну, трифакторного протоколу автентифікації та алгоритмів машинного навчання [20, 21].

В багаторівневій структурі інтелектуалізації об'єктів інфраструктури (рис. 1) безпровідні технології зв'язку є одним з функціональних рівнів КФС, який призначений для обміну інформацією між фізичним простором (інтернетом речей) та кібернетичним простором (комп'ютерною системою) у процесі відбирання інформації від фізичних об'єктів та управління їх станом на основі оброблення даних, аналізу й ухвалення рішення. В парадигмі "багаторівнева структура КФС – багаторівнева інформаційна безпека" (рис. 2) безпровідні технології зв'язку є сегментом захищеного комунікаційного середовища. Для забезпечення захищеного обміну інформацією в багаторівневій КФС актуальною є комплексна модель безпеки безпровідних технологій зв'язку (рис. 4), яка пов'язана з ієрархічною моделлю безпеки інтернету речей на транспортному рівні (рис. 3). Для комплексної моделі характерні: 1) єдина функціональна структура захисту інформації – зовнішня безпека, внутрішня безпека та політика інформаційної безпеки; 2) спеціалізована структура КСБ на основі концепції "об'єкт – загроза – захист", зумовлена комплексом загроз для об'єктів інфраструктури суспільства: "розумної екології", "розумної освіти", "розумної енергетики", "розумної транспортної системи".

Зовнішній рівень безпеки безпровідних технологій забезпечує система охорони периметра об'єкта інтелектуалізації, якій властиві відповідні критерії захисту та ступінь складності. Основними технологіями охорони периметра, спрямованої на протидію загрозам несанкціонованого доступу до ресурсів об'єкта інтелектуалізації, є: камери відеоспостереження, системи контролю доступу, електронні замки, біометричні системи розпізнавання. Внутрішній рівень безпеки безпровідних технологій зумовлюють категорії загроз, класифіковані за різними ознаками, серед яких загрози за природою виникнення: об'єктивні (природні), суб'єктивні (штучні); серед суб'єктивних загроз виділяють – випадкові і цілеспрямовані. Основні завдання безпеки інтелектуальних технологій пов'язані з протидією цілеспрямованим загрозам.

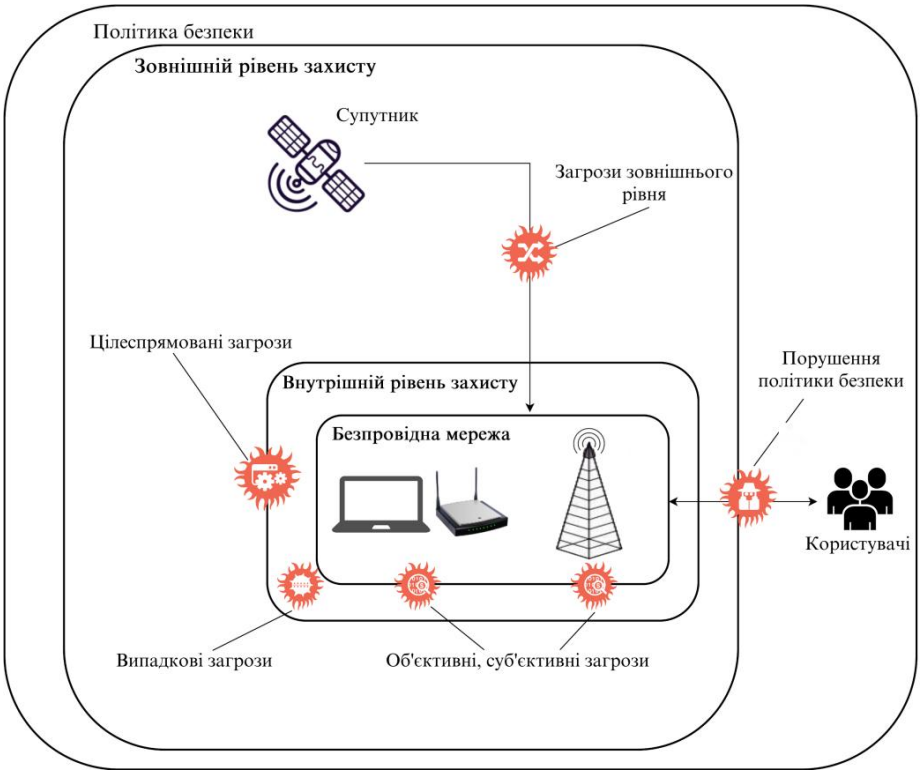

Рис. 4. Комплексна модель безпеки безпровідних технологій зв'язку

7. Результати дослідження

Запропоновані результати наукових досліджень за вектором безпеки кіберфізичних технологій згідно з концепцією Індустрія 4.0 є методологічними, оскільки охоплюють: системний підхід до безпечної інтелектуалізації об'єктів інфраструктури, багаторівневу парадигму безпеки кіберфізичних систем, розвиток моделей безпеки інтернету речей та безпровідних комунікаційних систем у просторі технологій кібербезпеки. Основними рівнями впровадження запропонованих результатів наукових досліджень є безпековий сегмент галузевої інфраструктури, а також навчальний процес за напрямом кібербезпека та захист інформації.

Висновки

Запропоновано багаторівневу структуру безпечної інтелектуалізації об'єктів інфраструктури суспільства, яка є основою для створення методологічного підходу до безпечного відбору інформації, захищеного обміну даними; безпечної обробки та управління станом об'єктів. Створено парадигму комплексної системи безпеки кіберфізичної системи – інструментарію безпечної інтелектуалізації об'єктів інфраструктури, що є підґрунтям для побудови моделей безпеки технологій фізичного простору, комунікаційного середовища, кібернетичного простору за впливу загроз конфіденційності, цілісності, доступності. Розвинуто безпеку інтернету речей та безпровідних технологій на рівні ієрархічної і комплексної моделей відповідно до ймовірних загроз, що забезпечує безпечний обмін інформацією в багаторівневій кіберфізичній системі.

Список літератури

1. Schwab Klaus. The Fourth Industrial Revolution. Geneva: World Economic Forum, 2016. Available at: https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-he_Fourth_Industrial_Revolution_Klaus_S.pdf (Accessed: 17 March 2024).

2. Gajdzik Bozena. Grabowska Sandra and Saniuk Sebastian. A Theoretical Framework for Industry 4.0 and Its Implementation with Selected Practical Schedules // Energies 2021, 14, 940, DOI: 10.3390/en14040940

3. Khan Firoz, Kumar R. Lakshmana, Kadry Seifedine, Nam Yunyoung, Meqdad Maytham N. Cyber physical systems: A smart city perspective // International Journal of Electrical and Computer Engineering (IJECE). Vol. 11. No. 4. August 2021. Pp. 3609–3616. DOI: 10.11591/ijece.v11i4.pp3609-3616

4. Yaacoub Jean-Paul A., Salman Ola, Noura Hassan N., Kaaniche Nesrine, Chehab Ali, Malli Mohamad. Cyber-physical systems security: Limitations, issues and future trends, Microprocessors and Microsystems, Volume 77, 2020, 103201, ISSN 0141-9331. DOI: 10.1016/j.micpro.2020.103201

5. Sandberg H. (2020). Cyber-Physical Security. In: Baillieul J., Samad T. (eds). Encyclopedia of Systems and Control. Springer, London. DOI: 10.1007/978-1-4471-5102-9_100112-1

6. Opirskyy I., Tyshyk I., Susukailo V. Evaluation of the Possibility of Realizing the Crime of the Information System at Different Stages of TCP/IP (2021) 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies, AICT 2021 – Proceedings, pp. 261–265, Cited 0 times. DOI: 10.1109/AICT52120.2021.962893.

7. Maksymovych V., Nyemkova E., Justice C., Shabatura M., Harasymchuk O., Lakh Y., Rusynko M. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics. (2022), 11(13):2039. DOI: 10.3390/electronics11132039

8. Lombardi M., Pascale F., Santaniello D. Internet of Things: A General Overview between Architectures, Protocols and Applications. Information 2021, 12(2), 87. DOI: 10.3390/info12020087

9. Wu C. K. Internet of Things Security. Architectures and Security Measures. Advances in Computer Science and Technology (In cooperation with the China Computer Federation (CCF). Springer, Singapore, 2021. 245 p. DOI: 10.1007/978-981-16-1372-2

10. Gupta N., Garg U. (2022). A Proposed IoT Security Framework and Analysis of Network Layer Attacks in IoT. In: Sharma T. K., Ahn C. W., Verma O. P., Panigrahi B. K. (eds). Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, Vol. 1380. Springer, Singapore. DOI: 10.1007/978-981-16-1740-9_9

11. Mykytyn H. V. Complex security system of cyber-physical system "iPhone – Wi-Fi, Bluetooth – sensors" / V. B. Dudykevych, G. V. Mykytyn, A. I. Rebets // Information processing systems. 2017. No. 2 (148). Pp. 84–87. DOI: 10.30748/soi.2017.148.16 [In Ukrainian].

12. Dudykevych V. B. ZigBee, Wi-Fi and Bluetooth wireless sensor networks in cyber-physical systems: the "object – threat – protection" concept based on the OSI model / V. B. Dudykevych, H. V. Mykytyn, A. I. Rebets, M. V. Melnyk // Information processing systems. 2019. Issue 2 (157). Pp. 114–120. DOI: 10.30748/soi.2019.157.16 *[In Ukrainian].*

13. Osterhage W. Wireless Network Security: Second Edition. CRC Press, 2018. 202 p. DOI: 10.1201/9781315106373

14. Sako K., Tippenhauer N. O. (eds.) Applied Cryptography and Network Security. ACNS 2021. Lecture Notes in Computer Science, vol. 12726. Springer, Cham, 2021. 482 p. DOI: 10.1007/978-3-030-78372-3

15. Chakraborty M., Jha R. K., Balas V. E., Sur S. N., Kandar D. (eds.) Trends in Wireless Communication and Information Security. Lecture Notes in Electrical Engineering, Vol. 740. Springer, Singapore, 2021. 416 p. DOI: 10.1007/978-981-33-6393-9

16. Nazir R., Laghari A. A., Kumar K. et al. Survey on Wireless Network Security. Archives of Computational Methods in Engineering (2021). DOI: 10.1007/s11831-021-09631-5

17. Zatserkovnyi V. I., Oberemok N. V., Tishaiev I. V., Kazanyuk T. A. Using of GIS technologies and remote sensing tools for monitoring of water objects // Science-Based Technologies. No. 1 (33), 2017. Pp. 78 88. DOI: 10.18372/2310-5461.33.11563 [In Ukrainian]

18. Kropyvnytskyi V., Pavlyshyn M., Chumak V. Highly mobile environmental monitoring laboratory. [Electronic resource]. Available at: https://ns-plus.com.ua/2017/06/13/vysokomobilna-laboratoriya-ekologichnogo-monitoryngu (Accessed: 17 March 2024). [In Ukrainian]

19. Information security in the environment of wireless sensor networks: a monograph / M. B. Aleksander, S. M. Balaban, M. P. Karpinskyi, S. A. Raiba, V. M. Chyzh. Ternopil: publishing house Ivan Puluj TNTU, 2016. 160 p. Available at: https://elartu.tntu.edu.ua/bitstream/123456789/18287/1/mon_wsn.pdf (Accessed: 17 March 2024). [In Ukrainian]

20. Awan S., Javaid N., Ulla, S., Khan A. U., Qamar A. M., Choi J.-G. Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. Sensors 2022, 22, 411. DOI: 10.3390/s22020411

21. Zhu L., Xiang H., Zhang K. A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks. Symmetry 2022, 14, 46. DOI: 10.3390/sym14010046

SECURITY METHODOLOGY OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS IN INTELLECTUALIZATION OF INFRASTRUCTURE OBJECTS

V. Dudykevych, H. Mykytyn, L. Bortnik, T. Stosyk

Lviv Polytechnic National University,
Information Security Department

A multi-level structure of safe intellectualization of society's infrastructure "objects – cyber-physical systems" in the functional space "selection – exchange of information – processing – management" is proposed according to the profiles – confidentiality, integrity, availability for "smart environmental monitoring", "smart education", "smart energy", "intelligent transport system" and other subject areas.

The multi-level structure "objects – cyber-physical systems" of safe intellectualization is revealed by the paradigm "multi-level cyber-physical system – multi-level information security", which is the basis for building complex security systems of technologies of physical space, communication environment and cyberspace.

A hierarchical model of Internet of Things security is built based on a three-layer architecture and the concept of "object – threat – protection". The complex security model of the wireless communication environment of cyber-physical systems for segments of the intellectualization of society's infrastructure is analysed. The presented methodology of safe processes of intellectualization allows the implementation of complex security systems of technologies for the functioning of society's infrastructure objects.

Keywords: intellectualization, information security, objects, cyber-physical system, multi-level structure, security paradigm, Internet of Things, hierarchical model, complex model.