УДК 004.056 DOI: 10.30748/soi.2019.157.16

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

Національний університет "Львівська політехніка", Львів

БЕЗПРОВІДНІ СЕНСОРНІ МЕРЕЖІ ZIGBEE, WI-FI ТА BLUETOOTH В КІБЕРФІЗИЧНИХ СИСТЕМАХ: КОНЦЕПЦІЯ "ОБ'ЄКТ – ЗАГРОЗА – ЗАХИСТ" НА ОСНОВІ МОДЕЛІ OSI

Розглянуто інформаційну безпеку сенсорних мереж Zigbee, Wi-Fi та Bluetooth згідно моделі OSI у просторі "рівень OSI – функції – протоколи" на основі концепції "об'єкт – загроза – захист" та нормативного забезпечення, які системно створюють підхід до побудови комплексних систем безпеки сенсорного безпровідного комунікаційного середовища (КС) кіберфізичних систем (КФС) за профілями конфіденційність – цілісність – доступність, що забезпечує безпечні процеси автоматизації об'єктів промислової інфраструктури України та інтеграції в міжнародний інтелектуальний простір.

Ключові слова: *сенсорна мережа, Zigbee, Wi-Fi, Bluetooth, кіберфізична система, модель OSI, інформаційна безпека, концепція "об'єкт – загроза – захист".*

Вступ

Постановка проблеми. Проект Концепції інформаційної безпеки (ІБ) України розгортає основні засади забезпечення безпеки інформаційних і телекомунікаційних систем, які сьогодні реалізують процеси інтелектуалізації суспільства [1]. Кіберне-тичний, комунікаційний, фізичний сегменти інтелектуального простору представлені багаторівневими кіберфізичними системами (КФС), функціональне призначення яких – контроль стану об'єктів, передавання та обробка інформації, управління фізичним середовищем. Нова парадигма "багаторівнева КФС – багаторівнева безпека" розкриває взаємодію КФС та Інтернет речей у напрямі автоматизації промислових комплексів, що розкриває перспективи розвитку безпечних розумних об'єктів, міст, країн [2]. Інформаційна безпека безпровідних сенсорних мереж *ZigBee*, *Wi-Fi*, *Bluetooth* – один з критеріїв забезпечення комплексної безпеки КФС.

Аналіз останніх досягнень і публікацій. Трикомпонентна структура програми ЄС з досліджень та інновацій "передова наука – індустріальне лідерство – соціальні виклики" за Рамковою програмою "Горизонт – 2020" та концепція майбутньої промисловості "Індустрія 4.0" розгортають взаємозв'язок кіберфізичних систем з промисловим Інтернетом, Інтернет речей, що сприяє розгортанню процесів міжнародної інтелектуалізації. Одним з підходів забезпечення безпечної інтелектуалізації є побудова комплексних систем безпеки (КСБ) багаторівневої КФС. Розроблення КСБ КФС згідно профілів безпеки (ISO/IEC 15408) є запитом на забезпечення захисту інформації в безпровідному сенсорному середовищі *ZigBee* (IEEE 802.15.4), *Wi-Fi* (IEEE 802.11), *Bluetooth* (IEEE 802.15.1) [3].

У монографії [4] проаналізовано: загрози інформаційним ресурсам в системах з безпровідними сенсорними мережами; методи контролю та візуалізації параметрів функціонування сенсорної мережі; запропоновано методи моделювання безпровідних сенсорних мереж, які сприяють розробленню їх апаратного і програмного забезпечення, що уможливлює реалізацію гнучкого моніторингу та виявлення пошкоджених елементів сенсорних мереж. В працях [5–6]: проаналізовано проблемні ділянки систем захисту сенсорних мереж; систематизовано класифікацію різних типів атак; запропоновано класифікацію механізмів забезпечення безпеки з метою мінімізації потенційних збитків від атак. В роботі [7] проаналізовано: основні вимоги до функціональної безпеки сенсорних мереж згідно стандартів МЕК 61508 та МЕК 61511; підходи до забезпечення інформаційної безпеки безпровідних сенсорних мереж. В праці [8]: представлено безпровідні сенсорні мережі як основну технологію, що дозволяє Інтернет речей; проведено аналіз вимог до шифрування, аутентифікації, відкритих ключів та управління ключами в безпровідних сенсорних мережах; розглянуто проблему нових протоколів маршрутизації сенсорних мереж. Стаття [9] розгортає: основні механізми безпеки, їх вплив на найпопулярніші протоколи і стандарти, що використовуються в безпровідних сенсорних мережах; аналіз атак мережевого рівня. Нову таксономію для атак на сенсорні мережі, які використовуються в промисловому контролі, управлінні трафіком, автоматизації житла, прогнозуванні погоди т.і. сферах, розглянуто в роботі [10]. Узагальненню питань безпеки безпровідних сенсорних мереж та проблем, які пов'язані з їх вирішенням, присвячена праця [11]. В роботі [12] проведено визначення ресурсних обмежень та енер-

гетичних проблем безпровідних сенсорних мереж та проаналізовано ефективні алгоритми та протоколи безпеки. Для протидії зростанню загроз безпеки і атак, окрім існуючих традиційних механізмів безпеки, використовують безпровідні сенсорні мережі з програмним забезпеченням [13]. З метою забезпечення вимог безпеки сенсорних мереж в роботі [14] розглянуто різні підходи до їх безпечного функціонування відповідно до комплексу атак та реалізації методик протидії.

Розглянуті наукові праці представляють аналіз методів та засобів захисту інформації в безпровідних сенсорних мережах. Застосування принципів системності в побудові КСБ сенсорних мереж *ZigBee*, *Wi-Fi* та *Bluetooth* на основі моделі OSI є розвитком підходів до ефективного застосування технологій безпеки безпровідного комунікаційного середовища кіберфізичних систем.

Мета статті. Метою роботи є створення концепції "об'єкт – загроза – захист" для безпровідного комунікаційного середовища КФС *ZigBee*, *Wi-Fi* та *Bluetooth* згідно моделі OSI та нормативного забезпечення.

Виклад основного матеріалу

1. Концепція "об'єкт – загроза – захист" на основі моделі OSI для сенсорної мережі ZIGBEE

Прикладний рівень. Мережа / протокол: APL (APS, ZDO і Application Objects) ZigBee. ***Функції:*** передача повідомлень; виявлення пристроїв; визначення ролі пристроїв. ***Загрози:*** використання безкоштовних ресурсів та програм невідомого походження; недоліки програмного забезпечення (ПЗ); наявність backdoors; обхід стандартних засобів управління безпекою; недостатній контроль засобів захисту за принципом "все або нічого", в результаті чого або надмірний/ недостатній доступ до мережі; надмірно ускладнений механізм контролю безпеки; збої ПЗ при великих навантаженнях. ***Захист:*** контроль на рівні програм визначає і забезпечує доступ до ресурсів; простий та прозорий механізм забезпечення безпеки, з метою уникнення складностей у конфігуруванні; реалізація криптографічного та антивірусного захисту даних.

Рівень представлення. Функції: здійснення організації даних, що передаються від прикладного рівня у мережу; забезпечення уніфікації даних при їх обміні між платформами із різними схемами кодування; контроль за стисненням та шифруванням даних. ***Загрози****:* погана обробка даних може призвести до збою програми; ненавмисне або необачне використання зовнішніх даних, що вводяться в контексті управління, може призвести до віддаленої маніпуляції або витоку інформації; криптографічні недоліки можуть бути використані для обходу захисту конфіденційності. ***Захист:*** ретельна перевірка даних, що вводяться до програми; контроль дій користувачів та функцій управління; ретельний і безперервний огляд рішень криптографії для забезпечення поточних завдань безпеки до загрози, що постійно оновлюються.

Сеансовий рівень. Функції: сприяння в обміні інформацією шляхом встановлення, підтримки, синхронізації, управління та завершення з'єднання з можливою ідентифікацією та аутентифікацією сторін. ***Загрози:*** слабкі або відсутні механізми аутентифікації; передача під час сеансу інформації, такої як ім'я користувача і пароль у відкритому вигляді, дозволяє її перехоплення та несанкціоноване використання; ідентифікація сеансу може бути предметом підміни і викрадення, витік інформації на основі невдалих спроб аутентифікації; здійснення атаки на облікові дані для доступу в разі необмеженої кількості спроб на встановлення сеансу. ***Захист:*** зашифрований обмін і зберігання паролів; обмежений термін дії для паролів та повноважень користувачів; захист інформації про ідентифікацію сеансу за допомогою криптографічних засобів; обмеження невдалих спроб встановлення сеансу за допомогою механізму синхронізації, а не блокування.

Транспортний рівень. Функції: здійснює доставку пакетів та дейтаграм від відправника до одержувача; орієнтований на підвищення продуктивності передачі інформації. ***Загрози****:* неправильна передача пакетів; відмінності в реалізації транспортного протоколу дозволяють здійснити несанкціонований доступ; перевантаження транспортного рівня за рахунок великої кількості звернень до номерів портів обмежує можливості для ефективної фільтрації трафіку; механізми передачі пакетів можуть бути предметом підміни і атаки на основі сформованих пакетів і призводити до руйнування або захоплення контролю над мережею. ***Захист:*** жорсткі правила брандмауера обмежують доступ до певних протоколів передачі інформації, таких як номер портів TCP/UDP; перевірка брандмауером пакетів з урахуванням аналізу вмісту та з'єднання дозволяє закрити доступ до мережі шкідливим пакетам; посилення механізмів ідентифікації з'єднання, щоб уникнути нападу і захоплення контролю над мережею.

Мережевий рівень. Мережа / протокол*:* NWK ZigBee. ***Функції:*** безпека, маршрутизація; реєстрація в мережі нового пристрою і виключення його з мережі; забезпечення безпеки при передачі фреймів; вказівка маршруту фрейма до місця призначення; прокладка маршрутів між пристроями в мережі; виявлення в мережі найближчих сусідів; запам'ятовування необхідної інформації про сусідні вузли. ***Загрози:*** підміна маршруту – поширення

неправдивої топології мережі; підміна ір-адреси – джерело помилкового рішення після дії шкідливих пакетів; проблеми одноразової ідентифікації. ***Захист:*** застосування політики управління маршрутами – жорсткі фільтри маршрутів і анти-спуфінг; використання міжмережевих екранів із потужною політикою фільтрації; моніторинг програмного забезпечення, для мінімізації можливих зловживань.

Канальний рівень. Мережа / протокол*:* LLC IEEE 802.15.4; SSCS IEEE 802.15.4; MAC IEEE 802.15.4. ***Функції:*** CSMA/CA, передача маячків; синхронізація; формування та доставка кадру без помилок. ***Загрози****:* підміна MAC-адреси; обхід технологій VLAN; використання помилок алгоритму; spanningtree для передачі пакетів у нескінченний цикл; несанкціоноване підключення до мережі; затоплення комутаторами всіх портів VLAN. ***Захист:*** фільтрація MAC-адрес; не використовувати мережі VLAN для захисту інформації; фізична ізоляція різних зон мережі за допомогою брандмауерів; бездротові мережі необхідно захищати використанням вбудованого шифрування, аутентифікації та фільтрації MAC-адрес.

Фізичний рівень. Мережа / протокол*:* PHY IEEE 802.15.4. ***Функції:*** фізичний зв'язок між кінцевими робочими станціями. ***Загрози****:* втрата потужності; фізичні крадіжки даних і устаткування; фізичне пошкодження або знищення даних і устаткування; несанкціоновані зміни у функціональному середовищі (передачі даних, змінних носіїв, додавання / видалення ресурсів); вимкнення фізичних каналів передачі даних; приховане перехоплення даних з клавіатури та інших засобів введення інформації. ***Захист:*** закриття периметру і корпусів мережі; електронний механізм блокування для реєстрації та авторизації; відео та аудіо спостереження; застосування pin-кодів і паролів; біометричні системи аутентифікації; електромагнітне екранування.

Нормативне забезпечення**:** IEEE Std. 802.15.4; ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв`язок відкритих систем. Базова еталонна модель. Частина 1. Еталонна модель; ДСТУ ISO 7498-2:2004 Системи оброблення інформації. Взаємозв`язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації; ISO/IEC 27033-1:2009. Information technology. Security techniques. Network security. Part 1: Overview and concepts (Інформаційна технологія. Методи захисту. Захист мережі. Частина 1. Огляд та концепції); ISO/IEC 27033-2:2012. Information technology. Security techniques. Guidelines for the design and implementation of network security (Інформаційна технологія. Методи захисту. Керівництво для розробки та впровадження захисту мережі).

2. Концепція "об'єкт – загроза – захист" на основі моделі OSI для сенсорної мережі WI-FI

Прикладний рівень. *Функції:* верхній рівень моделі, що забезпечує взаємодію користувацьких додатків з мережею. *Загрози:* несанкціоноване одержання прав на виконання дій з інформацією; спотворення інформації (навмисне чи ні); припинення виконання необхідних функцій. *Захист:* ідентифікація та аутентифікація користувачів при спробі встановлення з'єднань через МЕ; перевірка достовірності інформації, переданої через шлюз; розмежування доступу до ресурсів внутрішньої і зовнішньої мереж; фільтрація і перетворення потоку повідомлень, наприклад динамічний пошук вірусів і прозоре шифрування інформації; реєстрація подій, реагування на поставлені події, а також аналіз зареєстрованої інформації та генерація звітів; кешування даних, запитуваних із зовнішньої мережі.

Рівень представлення. Функції: перетворення протоколів і кодування / декодування даних; запити додатків, отримані з прикладного рівня, на рівні уявлення перетворюються у формат для передачі по мережі, а отримані з мережі дані перетворюються в формат додатків; стиснення / розпакування або шифрування / дешифрування, а також перенаправлення запитів іншому мережному ресурсу, якщо вони не можуть бути оброблені локально. ***Загрози:*** несанкціоноване одержання прав на виконання дій з інформацією; спотворення інформації (навмисне чи ні); припинення виконання необхідних функцій. ***Захист:*** ідентифікація та аутентифікація користувачів при спробі встановлення з'єднань через МЕ; перевірка достовірності інформації, переданої через шлюз; розмежування доступу до ресурсів внутрішньої і зовнішньої мереж; фільтрація і перетворення потоку повідомлень, наприклад динамічний пошук вірусів і прозоре шифрування інформації; реєстрація подій, реагування на поставлені події, а також аналіз зареєстрованої інформації та генерація звітів; кешування даних, запитуваних із зовнішньої мережі.

Сеансовий рівень. Функції: забезпечення підтримання сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час; управляння створенням / завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків. ***Загрози:*** спотворення інформації; несанкціоноване завершення, пере адресація сеансу; виведення з ладу сеансових шлюзів; підключення до сеансів несанкціонованих додатків; аналіз відкритої інформації в сеансах; ініціалізація сеансу з метою перехоплення даних. ***Захист:*** ідентифікація учасників сеансу; перевірка автентичності клієнта та сервера; фільтрація пакетів сеансів; приховування внутрішніх адрес із застосуванням сеансового шлю-

зу, який відображає внутрішні адреси локальної мережі.

Транспортний рівень. ***Функції:*** забезпечення додаткам необхідного ступеня захисту при доставці повідомлень. ***Загрози****:* аналіз регулярності трафіку і посилка паралельних дублікатів повідомлень по інших шляхах, використовуваних на даному рівні. ***Захист:*** шифрування даних; протоколи TLSP.

Мережевий рівень. Функції: забезпечує наскрізну передачу пакету, розраховуючи його маршрут; присвоює пакетам IP-адресу. ***Загрози:*** читання, модифікація, знищення, дублювання даних; переорієнтація; маскування під інший вузол. ***Захист:*** шифрування даних; протокол IPSEC.

Канальний рівень. Мережа / протокол: підрівень LLC; підрівень MAC. ***Функції:*** управління доступом до середовища передачі; забезпечення пересилання кадрів між будь-якими двома пристроями бездротової мережі. ***Загрози:*** маніпуляція бітами (bit-flipping атаки); атака за словником на wpa / wpa2 psk; відмови в обслуговуванні; злом шифрування. ***Захист:*** методи шифрування; методи аутентифікації; методи обмеження доступу.

Фізичний рівень. Мережа / протокол*:* підрівень PCLD; підрівень PMD. ***Функції:*** безпровідна передача; оцінка стану ефіру. ***Загрози:*** активність у неробочий час; інтерференція; неправильно конфігурований клієнт; відмови в обслуговуванні. ***Захист:*** фізичне відключення точок доступу; моніторинг всіх підключень до мережі; mac фільтрація; технологія vpn.

Нормативне забезпечення**:** IEEE Std. 802.11; ДСТУ ISO/IEC 7498-3:2004 Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 3. Найменування та адресація; НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу; ISO/IEC 27033-3:2010. Information technology. Security techniques. Network security. Reference networking scenarios. Threats, design techniques and control issues (Інформаційна технологія. Методи захисту. Захист мережі. Рекомендовані сценарії мережі. Загрози); ISO/IEC 27033-4:2014. Information technology. Security techniques. Network security. Securing communications between networks using security gateways (Інформаційна технологія. Методи захисту. Захист мережі. Використання захисних шлюзів для безпеки з'єднання між мережами).

3. Концепція "об'єкт – загроза – захист" на основі моделі OSI для сенсорної мережі BLUETOOTH

Фізичний рівень. Мережа / протокол*:* LMP (Link Management Protocol); HCI (Host/controller interface); AVRCP (A/V Remote Control Profile); L2CAP (Logical Link Control and Adaptation Protocol); SDP (Service Discovery Protocol); RFCOMM (Radio Frequency Communications); BNEP (Bluetooth Network Encapsulation Protocol); AVCTP (Audio/Video Control Transport Protocol); AVDTP (Audio/Video Distribution Transport Protocol); TCS (Telephony Control Protocol). ***Функції:*** встановлення та управління радіо з'єднанням між двома пристроями; узгодження контролерів; визначення зв'язку між стеком хоста і контролером; управління звуковим потоком через Bluetooth; мультиплексування локальних з'єднань між двома пристроями, що використовують різні протоколи більш високого рівня; фрагментування і перезбирання пакетів; виявлення послуг, що надаються іншими пристроями; визначення параметрів послуг; заміна кабелю; створення віртуального послідовного потоку даних; емуляція керуючих сигналів RS-232; передача даних з інших стеків протоколів через канал L2CAP; передача IC пакетів в профілі Personal Area Networking; передача команд по каналу L2CAP в профілі аудіо / Video Remote Control; передача стерео звуку по каналу L2CAP в профілі Advanced Audio Distribution; визначення сигналів управління викликом для встановлення голосових з'єднань і з'єднань для передачі даних в профілі Cordless Telephony. ***Загрози***: підміна пристрої (атака людина-в-середині); створення перешкод в діапазоні роботи пристроїв; виведення з ладу контролерів; перехоплення пакетів; підміна контролера; відправка помилкових статусів підключення; спотворення звукового потоку; перехоплення голосових повідомлень; помилки мультиплексування з'єднань; помилки фрагментування / перезбирання пакетів; несанкціоноване використання послуг; несанкціоновані зміни послуг; виникнення помилок в потоці даних; збої емуляції; перехоплення потоку даних; перехоплення даних; IP-спуфінг; флудинг; сніферінг; несанкціонована зміна команд; заміна пристрою; спотворення звуку; обрив зв'язку; переадресація викликів; хибне визначення сигналів. ***Захист:*** аутентифікація, ідентифікація, авторизація пристроїв мережі; фільтрація сигналу; контроль доступу апаратурі; шифрування пакетів; шифрування статусів; аутентифікація, ідентифікація, авторизація контролерів; застосування завадостійкого кодування; скремблювання голосових повідомлень; шифрування повідомлень; застосування коректувальної надлишковості; ведення протоколів помилок; аутентифікація, ідентифікація, авторизація користувачів; контроль зміни параметрів послуг; автоматичний аналіз і виправлення помилок; застосування преемуляції; шифрування потоку даних; установка обмеження пакетів; фільтрація даних; шифрування даних; ускладнення синтаксису команд; синхронна авторизація; зменшення затримки повторного підключення; використання кодеків із стисненням; багатоетапне визначення сигналів.

Нормативне забезпечення: IEEE 802.15.1;НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу; ДСТУ 3043-95 Системи оброблення інформації. Телеобробка даних і комп'ютерні мережі. Терміни та визначення; ДСТУ ISO/IEC TR 13335-1:2001 Інформаційні технології. Настанова для керування ІТ безпекою. Частина 5. Настанова керування безпекою мережі; ISO/IEC 27033-5:2013. Information technology. Security techniques. Network security. Securing communications across networks using VPN (Інформаційна технологія. Методи захисту. Захист мережі. Використання віртуальних приватних мереж для захисту з'єднання).

Висновки

В роботі висвітлено концептуальний підхід до забезпечення ІБ безпровідних сенсорних мереж *ZigBee*, *Wi-Fi*, *Bluetooth* на основі моделі OSI згідно державних та міжнародних стандартів. Концепція "об'єкт – загроза – захист" є універсальною у просторі безпеки кіберфізичних систем, що уможливлює її реалізацію на рівні створення КСБ комунікаційного середовища КФС відповідно до топології мереж та їх ділянок.

Список літератури

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

2. Дудикевич В.Б. Квінтесенція безпеки кіберфізичних систем / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець // Інформаційні системи і мережі. – 2018. – № 887. – С. 58-69.

3. Security of Cyber-Physical Systems from Concept to Complex Information Security System / V. Dudykevych, G. Mykytyn, T. Kret, A. Rebets // Advances in Cyber-Physical Systems. – Volume 1, Number 2 (2016). – С. 67-75.

4. Інформаційна безпека в середовищі безпроводових сенсорних мереж: монографія / М.Б. Александер, С.М. Балабан, М.П. Карпінський, С.А. Райба, В.М. Чиж. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 160 с.

5. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О.Г. Корченко, М.Б. Алєксандер, Р.С. Одарченко, А. Алі Наджі, О.Ю. Петренко // Захист інформації. – 6 – 2016. – Том 18. – № 1. – С. 48-56.

6. Волошко С.В. Інформаційна безпека в безпроводових сенсорних мережах [Електронний ресурс] / С.В. Волошко, Д.О. Курца // Новітні інформаційні системи і технології. – 2018. – Випуск 9. – Режим доступу: http://journals.pntu.edu.ua/mist/article/view/1039/869.

7. Романов В.О. Вимоги до забезпечення функціональної та інформаційної безпеки бездротових сенсорних мереж / В.О. Романов, І.Б. Галелюка, В.О. Остапенко // Комп'ютерні засоби, мережі та системи. – 2017. – № 16. – С. 106-117.

8. Harsh Kupwade Patil. Wireless Sensor Network Security: The Internet of Things [Електронний ресурс] / Harsh Kupwade Patil, Thomas M.Chen // Computer and Information Security Handbook. – 2017. – Third Edition, Chapter 18. – P. 317-337. – Режим доступу: https://www.sciencedirect.com/science/article/pii/B9780128038437000181?via%3Dihub.

9. Tomić I. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols / I. Tomić, J.A. McCann // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 6. – P. 1910-1923.

10. Mabrook Al-Rakhami. Saleh Almowuena Wireless Sensor Networks Security: State of the Art [Електронний ресурс] / Mabrook Al-Rakhami, Saleh Almowuena. – 2018. – Режим доступу: https://arxiv.org/abs/1808.05272.

11. Wireless Sensor Network Security for Cyber-Physical Systems / Saqib Ali, Taiseera Al, BalushiZia, NadirOmar, Khadeer Hussain // Cyber Security for Cyber Physical Systems. Studies in Computational Intelligence. – 2018. – Vol. 768. – P. 35-63.

12. Wassim Itani. Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing / Wassim Itani, Ayman Kayssi, Ali Chehab // International Journal of Reliable and Quality E-Healthcare (IJRQEH). – 2016. – Vol. 5, Issue 2. – P. 1-30.

13. Tebogo Kgogo. Software defined wireless sensor networks security challenges // Tebogo Kgogo, Bassey Isong, Adnan M. Abu-Mahfouz // IEEE AFRICON. – 2017. – P. 1508-1513.

14. Waleed Al Shehri. A Survey On Security In Wireless Sensor Networks // International Journal of Network Security & Its Applications (IJNSA). – 2017. – Vol. 9, No. 1. – P. 25-32.

References

1. "*Proekt Koncepciji informacijnoji bezpeky Ukrajiny*" [*Draft Concept of Information Security of Ukraine*], available at: www.mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

2. Dudykevych, V.B., Mykytyn, Gh.V. and Rebecj, A.I. (2018), "Kvintesencija bezpeky kiberfizychnykh system" [Quantum safety of cybernetic systems], *Informacijni systemy i merezhi*, No. 887, pp. 58-69.

3. Dudykevych, V., Mykytyn, G., Kret, T. and Rebets, A. (2016), Security of Cyber-Physical Systems from Concept to Complex Information Security System, *Advances in Cyber-Physical Systems*, Vol. 1, No. 2, pp. 67-75.

4. Aleksander, M.B., Balaban, S.M., Karpinsjkyj, M.P., Rajba, S.A. and Chyzh, V.M. (2016), "*Informacijna bezpeka v seredovyshhi bezprovodovykh sensornykh merezh: monoghrafija*" [*Information security in a wireless sensor network environment: a monograph*], Vyd-vo TNTU imeni Ivana Puljuja, Ternopilj, 160 p.

5. Korchenko, O.Gh., Aljeksander, M.B., Odarchenko, R.S., Ali Nadzhi, A. and Petrenko, O.Ju. (2016), "Analiz zaghroz ta mekhanizmiv zabezpechennja informacijnoji bezpeky v sensornykh merezhakh" [Analysis of threats and mechanisms for providing information security in sensory networks], *Zakhyst informaciji*, Vol. 18, No. 1, pp. 48-56.

6. Voloshko, S.V. and Kurca, D.O. (2018), "Informacijna bezpeka v bezprovodovykh sensornykh merezhakh" [Information Security in Wireless Sensor Networks], *Novitni informacijni systemy i tekhnologhiji*, No. 9, available at: www.journals.pntu.edu.ua/mist/article/view/1039/869.

7. Romanov, V.O., Ghaleljuka, I.B. and Ostapenko, V.O. (2017), "Vymoghy do zabezpechennja funkcionaljnoji ta informacijnoji bezpeky bezdrotovykh sensornykh merezh" [Requirements for the provision of functional and informational security of wireless sensor networks], *Komp'juterni zasoby, merezhi ta systemy*, No. 16, pp. 106-117.

8. Harsh Kupwade Patil and Thomas M. Chen (2017), Wireless Sensor Network Security: The Internet of Things, *Computer and Information Security Handbook*, Chapter 18, pp. 317-337, available at: https://www.sciencedirect.com/science/article/pii/B9780128038437000181?via%3Dihub.

9. Tomić, I. and McCann, J.A. (2017), A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols, *IEEE Internet of Things Journal*, Vol. 4, No. 6, pp. 1910-1923.

10. Al-Rakhami, Mabrook and Almowuena, Saleh (2018), *Wireless Sensor Networks Security: State of the Art*, available at: https://arxiv.org/abs/1808.05272.

11. Saqib Ali, Taiseera Al, BalushiZia, NadirOmar and Khadeer, Hussain (2018), Wireless Sensor Network Security for Cyber-Physical Systems, *Cyber Security for Cyber Physical Systems. Studies in Computational Intelligence*, Vol. 768, pp. 35-63.

12. Wassim Itani, Ayman Kayssi and Ali Chehab (2016), Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing, *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, Vol. 5, Is. 2, pp. 1-30.

13. Tebogo Kgogo, Bassey Isong and Adnan M. Abu-Mahfouz (2017), Software defined wireless sensor networks security challenges, *IEEE AFRICON*, pp. 1508-1513.

14. Waleed Al Shehri (2017), A Survey On Security In Wireless Sensor Networks, *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 9, No. 1, pp. 25-32.

Надійшла до редколегії 16.04.2019
Схвалена до друку 21.05.2019

Відомості про авторів:

Дудикевич Валерій Богданович
доктор технічних наук професор
завідувач кафедри Національного університету
"Львівська політехніка",
Львів, Україна
https://orcid.org/0000-0001-8827-9920

Микитин Галина Василівна
доктор технічних наук професор
професор кафедри Національного університету
"Львівська політехніка",
Львів, Україна
https://orcid.org/0000-0003-4275-8285

Ребець Андрій Ігорович
аспірант Національного університету
"Львівська політехніка",
Львів, Україна
https://orcid.org/0000-0002-0310-517X

Мельник Мар'ян Володимирович
студент-магістрант Національного університету
"Львівська політехніка",
Львів, Україна
https://orcid.org/0000-0003-2156-4940

Information about the authors:

Valeriy Dudykevych
Doctor of Technical Sciences Professor
Head of Department
of Lviv Polytechnic National University,
Lviv, Ukraine
https://orcid.org/0000-0001-8827-9920

Galyna Mykytyn
Doctor of Technical Sciences Professor
Professor of Department
of Lviv Polytechnic National University,
Lviv, Ukraine
https://orcid.org/0000-0003-4275-8285

Andrii Rebets
Doctoral Student
of Lviv Polytechnic National University,
Lviv, Ukraine
https://orcid.org/0000-0002-0310-517X

Marian Melnyk
Graduate Student
of Lviv Polytechnic National University,
Lviv, Ukraine
https://orcid.org/0000-0003-2156-4940

БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ ZIGBEE, WI-FI И BLUETOOTH В КІБЕРФИЗИЧЕСКИХ СИСТЕМАХ: КОНЦЕПЦИЯ “ОБЪЕКТ – УГРОЗА – ЗАЩИТА” НА ОСНОВЕ МОДЕЛИ OSI

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

Рассмотрена информационная безопасность сенсорных сетей Zigbee, Wi-Fi и Bluetooth согласно модели OSI в пространстве “уровень OSI – функции – протоколы” на основе концепции “объект – угроза – защита” и нормативного обеспечения, которые системно создают подход к построению комплексных систем безопасности сенсорной беспроводной коммуникационной среды киберфических систем по профилям конфиденциальность – целостность – доступность, что обеспечивает безопасные процессы автоматизации объектов промышленной инфраструктуры Украины и интеграцию в международное интеллектуальное пространство.

***Ключевые слова**: сенсорная сеть, Zigbee, Wi-Fi, Bluetooth, киберфизическая система, модель OSI, информационная безопасность, концепция “объект – угроза – защита”.*

WIRELESS SENSOR NETWORKS ZIGBEE, WI-FI AND BLUETOOTH IN CYBER-PHYSICAL SYSTEMS: THE CONCEPTION “OBJECT – THREAT – DEFENCE” ON THE BASIS OF OSI MODEL

V. Dudykevych, G. Mykytyn, A. Rebets, M. Melnyk

The approach to provide information security of sensor networks based on Zigbee, Wi-Fi and Bluetooth developed in the article according to the OSI model in the space “OSI layer – functions – protocols” built on the conception “object – threat – defense” and standardization. The results of modern research on security concerns related to wireless sensor networks cover a wide range of information security methods and tools. The application of system analysis and modeling methods to create complex security system of sensor networks based on ZigBee, Wi-Fi and Bluetooth according to the OSI model allows to develop effective approaches to information security of cyber-physical system wireless communication environment. The results of the conception “object – threat – defense” applying to provide security of sensor networks based on ZigBee and Wi-Fi at the application, presentation, session, transport, network, data link and physical layers of the OSI model for the relevant protocols, functions, threats and protection are given. The basis of the conception is the standardization related to the abovementioned network technologies. The proposed conception of ZigBee, Wi-Fi and Bluetooth sensor networks security is important for secure communication establishment between physical and cybernetic layers of cyber-physical system during registered information transmission through the sensor network from physical objects to embedded computer with the purpose of data processing and object state identification, and, based on it, making the control decision. The obtained results can be used to create complex security systems for the communication environment of cyber-physical systems, which will ensure safe processes of automation of Ukrainian industrial infrastructure objects and integration into the international intellectual space. The developed models are universal in the space of information security of cyber-physics systems and they form a strategy for further practical research and application.

***Keywords:** sensor network, Zigbee, Wi-Fi, Bluetooth, cyber-physical system, OSI model, information security, object-threat-defense concept.*