УДК 004.054
DOI: 10.31673/2409-7292.2025.014428

Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М.

КОМПЛЕКСНА СИСТЕМА БЕЗПЕКИ ІНТЕЛЕКТУАЛЬНОЇ КІБЕРФІЗИЧНОЇ СИСТЕМИ МОНІТОРИНГУ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Стратегія кібербезпеки України передбачає розвиток методологічних підходів до безпеки інтелектуальних технологій для функціональної підтримки сегмента безпечного моніторингу надзвичайних ситуацій екосистеми регіонів України. Проведено аналіз останніх досліджень у напрямі розроблення архітектури кіберфізичних систем, створення моделей їх безпеки та практичної реалізації безпечних кіберфізичних систем в предметних сферах інфраструктури суспільства. Досліджено аспекти створення інтелектуальної кіберфізичної системи моніторингу параметрів надзвичайних ситуацій екосистеми регіону на основі універсальної платформи “архітектура інтелектуальної кіберфізичної системи – інтегральна модель безпеки – комплексна система безпеки”. Розглянуто багаторівневу архітектуру інтелектуальної кіберфізичної системи, яка уможливлює відбір параметрів надзвичайних ситуацій екосистеми регіону за впливу природних і техногенних факторів в просторі “контроль – обробка – аналіз – управління” і є основою для побудови інтегральної моделі її безпеки. Розгорнуто функціональність інтелектуальної кіберфізичної системи на рівні технологій: фізичного простору (давачів моніторингу – парникових газів, радіоактивних викидів, параметрів виявлення землетрусів; систем відеоспостереження надзвичайних ситуацій в режимі реального часу); комунікаційного середовища (безпровідних комунікаційних систем – LoRaWAN, GPS, LTE); кібернетичного простору (геоінформаційної системи, інформаційних ресурсів). На основі концепції “об’єкт – загроза – захист” запропоновано комплексні системи безпеки інтелектуальної кіберфізичної системи за впливу цілеспрямованих і випадкових загроз безпеці на зовнішньому і внутрішньому рівнях. Проаналізовано аспекти мандатної політики безпеки інтелектуальної кіберфізичної системи за основним профілем безпеки – конфіденційністю.

Ключові слова: інтелектуалізація, надзвичайні ситуації, екосистема регіону, моніторинг, кібербезпека, інтелектуальна кіберзична система, комплексні системи безпеки, мандатна політика безпеки.

Вступ

Сьогодні триває розвиток підходів до вирішення проблеми безпечного функціонування об’єктів інфраструктури України, зокрема критичної в умовах глобальних викликів світу. Актуальність вектору кібербезпеки висвітлена в: Індустрії 4.0, Кліматичному саміті COP 29 (вересень 2024 р., Азербайджан, Баку), дев’ятій Рамковій програмі “Горизонт Європа” (2021 – 2027 рр.) у частині впровадження технологій передової науки на основі системних і синергетичних принципів. Ефективним інструментарієм для розв'язання проблеми безпечної інтелектуалізації об’єктів інфраструктури суспільства за векторами Стратегії кібербезпеки України є інтелектуальні кіберфізичні системи та комплексні системи їх безпеки (КСБ) [1].

Аналіз літературних джерел

Кіберфізичні технології, як один з основних інструментаріїв моніторингу надзвичайних ситуацій регіону, розвиваються за векторами архітектури та кібербезпеки. Розглянемо деякі тенденції в Україні та на міжнародному рівні. Актуальним є розвиток застосування інтелектуальних кіберфізичних систем (ІКФС) у просторі Концепції Індустрії 4.0, зокрема із використанням елементів штучного інтелекту в промислових ІКФС для прийняття управлінського рішення в предметних сферах суспільства [2-5]. В роботі [6] розглянуто моделі й методи захисту інформації на основі багатоконтурного підходу безпечного функціонування інформаційних ресурсів в КФС. З метою забезпечення збереження конфіденційності та захисту цілісності інформації в КФС автор праці [7] представляє вимоги щодо застосування криптографічних засобів. Сьогодні розгортаються процеси взаємозв’язку архітектури та безпеки кіберфізичних технологій [8, 9], зокрема на концептуальному рівні згідно з парадигмою “багаторівнева ІКФС – багаторівнева безпека” [10], що знаходить впровадження такої моделі у сферу безпечного функціонування кіберфізичних енергосистем [11]. Продовжується розвиток архітектури КФС на рівні інтеграції обчислень, мереж та фізичних процесів та їх ефективне використання на міждисциплінарному рівні [12, 13]. В статті [14] представлено комплексний підхід до безпеки КФС на рівні “загрози – захист”, який охоплює простори: фізичний, кібернетичний, кіберфізичний.

Метою роботи є – розроблення методології безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій в умовах техногенних і природних факторів впливу згідно зі структурою "архітектура ІКФС – інтегральна модель безпеки – комплексна система безпеки", яка реалізує конструктивний алгоритм їх безпечного функціонування на основі концепції "об'єкт – загроза – захист".

Багаторівнева архітектура ІКФС моніторингу надзвичайних ситуацій

В контексті Регламенту моніторингу надзвичайних ситуацій (Regulations on the interaction of subjects of monitoring, surveillance, laboratory control and forecasting of emergencies, 2018), що виникають в умовах негативних факторів впливу техногенного характеру (викидів парникових газів, небезпечних шкідливих речовин, зокрема радіоактивних, аварій на електроенергетичних системах та в системах нафтогазового промислового комплексу т. і.) та природного (геофізичного, метеорологічного, медико-біологічного т. і.), актуальними є аспекти застосування ефективних інтелектуальних технологій у просторі "контроль – обробка – управління", серед яких багаторівневі кіберфізичні системи. На рисунку 1 представлена функціональна структура трирівневої ІКФС у взаємозв'язку з об'єктами дослідження, що характеризують параметри надзвичайних ситуацій, на рівні: фізичного простору – давачів відбору інформації про стан параметрів екосистем регіону; комунікаційного середовища (КС) – безпровідних мереж обміну даними; кібернетичного простору – геоінформаційної системи (ГІС) з виходом на WEB-додатки та аналітичний центр.

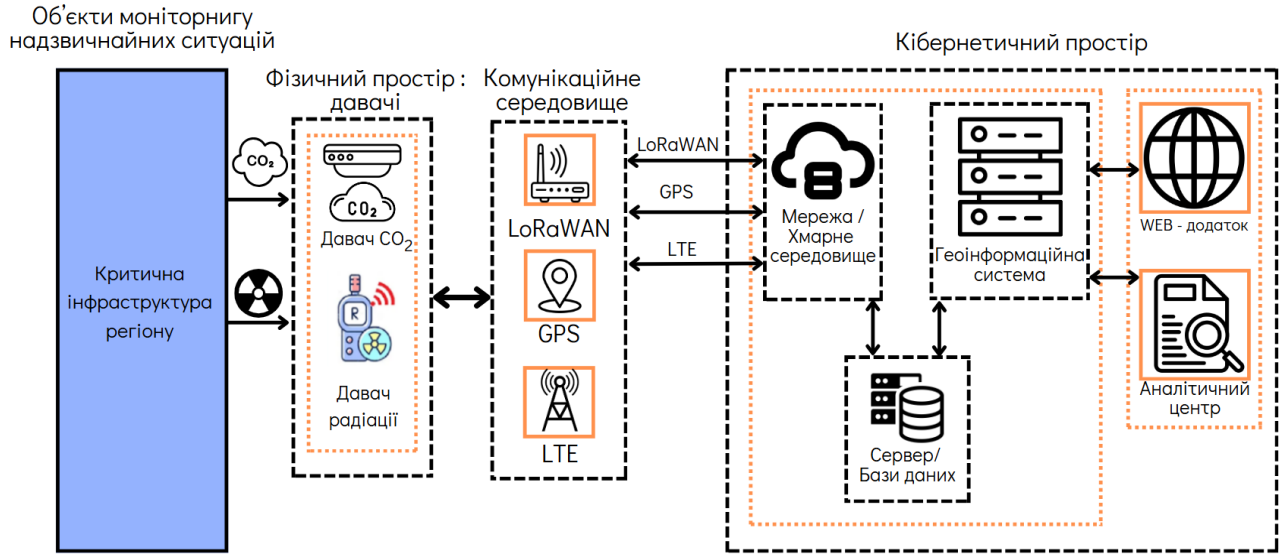

Рис. 1. Архітектура інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій регіону

Фізичний простір ІКФС. Розглянемо декілька давачів фізичного простору інтелектуальної кіберфізичної системи, які здійснюють відбір параметрів техногенного і природного впливу, що характеризують надзвичайні ситуації регіону (таблиця 1).

Комунікаційні системи безпровідного зв'язку ІКФС моніторингу надзвичайних ситуацій. Мережевий протокол LoRaWAN з великою дальністю дії ефективно застосовується для широкого покриття при мінімальному енергоспоживанні. Глобальна навігаційна супутникова система GPS дозволяє визначати місцеперебування об'єктів на поверхні Землі, що є важливим для ефективного моніторингу та реагування на надзвичайні ситуації. Технологія мобільного зв'язку LTE забезпечує високошвидкісне передавання даних у мобільних мережах, кращу продуктивність, високу пропускну здатність і меншу затримку сигналів.

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

Таблиця 1

Давачі ІКФС моніторингу параметрів надзвичайних ситуацій
за впливу природніх і техногенних факторів

Давач фізичного простору ІКФС	**Характеристики давачів фізичного простору ІКФС**
 Siemens Air Quality Sensor	Давач моніторингу парникових газів: викидів CO2 Протокол зв'язку: ZigBee Діапазон робочої температури: -10°C до +50°C Давач якості повітря: живлення від 12v тип живлення: 1 x CR123A
 БДБГ-310 (а); БДКС-310 (б)	Давачі моніторингу радіоактивних викидів: гамма-випромінювання Призначення: виявлення рівня іонізуючої радіації в середовищі; використання на АЕС, в медичних установах та інших об'єктах, де є ризик випадкового викиду радіації Характеристики: (а) від 0,04 мкЗв/год до 30,0 Зв/год (б) від 0,01 мкЗв/год до 30,0 Зв/год
 СД-2D	Давачі реєстрації параметрів виявлення землетрусів в регіоні Вимоги: можливість віддаленого моніторингу, наявність елементів безперебійного живлення та високої відмовостійкості Чутливість: 50mV/g Діапазон зондування: 0Hz ~ 180Hz
 Hikvision DS-2CD2T35FWD-I8	Камери відеоспостереження: моніторинг надзвичайних ситуацій регіону в режимі реального часу Поворот: від 0° до 360° Інтерфейс: RJ-45 Підтримка роздільних здатностей: 2688 × 1520, 2560 × 1440 Робоча напруга 12 В

Особливості застосування LoRaWAN: 1) низька швидкість передавання даних, що підходить для моніторингу стану давачів, зокрема у просторі моніторингу параметрів надзвичайних ситуацій, де не потрібне миттєве передавання великих обсягів інформації; 2) великий радіус дії, що дозволяє передавати дані на великі відстані і покривати великі площі з обмеженою кількістю базових станцій; 3) пристрої LoRaWAN мають дуже низьке енергоспоживання, що дозволяє їм працювати на одній батареї кілька років; 4) висока проникність сигналу, що забезпечує його проникнення навіть у щільно забудованих містах/ підземних спорудах; 5) підтримка шифрування AES-128 для безпечного обміну інформацією, забезпечення конфіденційності та аутентифікації.

Особливості застосування GPS-технології, зображеної на рисунку 2: 1) GPS-технологія складається з 24 супутників у високообертових орбітах; 2) наземні контрольні станції призначені для моніторингу та управління роботою супутників; 3) сучасні GPS-приймачі можуть надавати точність визначення місцеперебування об'єктів від кількох метрів до декількох сантиметрів; 4) GPS-приймачі розташовані в мобільних терміналах, автомобілях,

навігаційних пристроях тощо, отримують сигнали від супутників, визначають місцеперебування об'єктів.

Особливості застосування LTE: 1) LTE підтримує швидке масштабування мережі для підключення численних сенсорів і пристроїв, що забезпечує своєчасне отримання даних з місць подій та покращує ситуаційну обізнаність; 2) стандарт LTE забезпечує можливість адаптивного розподілу ресурсів, який дозволяє виділити необхідну пропускну здатність для критичних застосунків, таких як передавання відео/ даних з сенсорів, особливо у випадках з високим навантаженням на мережу; 3) використовує різні механізми шифрування та ідентифікації для забезпечення безпечного обміну даними в різних частотних діапазонах, включаючи: низькі (700 – 900 МГц), середні (1700 – 2100 МГц), високі (2.5 ГГц).

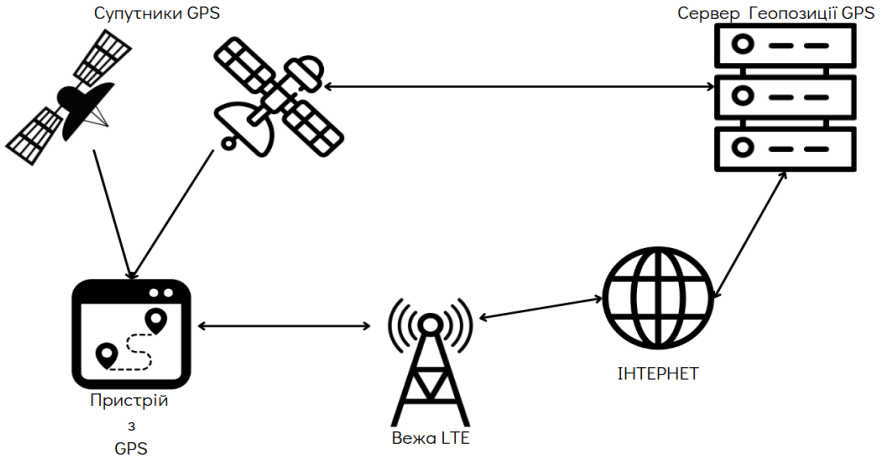

Рис. 2. Алгоритм функціонування комунікаційної технології GPS

Кібернетичний простір ІКФС: геоінформаційна система. Геоінформаційні системи (ГІС) є результатом розвитку традиційних інформаційних систем, що інтегрують високі технології для автоматизації процесів прийняття рішень, зокрема, на основі просторових даних. Вони використовуються для ефективного управління регіональними та територіальними даними з метою забезпечення: стратегічного планування, аналізу ризиків прийняття управлінських рішень.

Особливості застосування ГІС: можливість роботи зі слабкоструктурованими і динамічними просторовими даними; адаптивність та здатність до самонавчання; підтримка природномовного інтерфейсу для користувачів без технічних знань; здатність до вилучення знань на основі попереднього досвіду.

Компоненти ГІС включають базу знань, що забезпечує моделювання досліджуваної предметної сфери і механізми логічного виведення для підтримки рекомендацій у складних ситуаціях. Геоінформаційні системи класифікуються за: предметною сферою, ступенем автономності, адаптивністю, взаємодією з просторовими об’єктами та моделлю подання знань. На рисунку 3 представлена функціональна структура ГІС на рівні компонентів [15].

У функціональній структурі ГІС: інформаційно-довідкові функції забезпечують створення та ведення банків просторово-координованої інформації; консультаційно-експертні функції сприяють розв’язку задач обробки інформації; функції автоматизованого картографування уможливлюють створення високоякісних загальногеографічних і тематичних карт; функції просторового аналізу та моделювання і функції моделювання та прогнозування процесів розкривають специфіку функціональних завдань; функції підтримки прийняття рішень у циклі “планування – проектування – управління”; керуючі та транспортні функції оперативного прийняття рішень на управління; контрольні функції розгортають процеси оцінювання ефективності управлінських рішень.

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

Інтегральна модель та комплексні системи безпеки ІКФС моніторингу надзвичайних ситуацій екосистеми регіону

Інтегральна модель безпеки ІКФС моніторингу надзвичайних ситуацій екосистеми, що зображена на рисунку 4, є багаторівневою і представлена зовнішнім і внутрішнім рівнями технологій безпеки за впливу ймовірних цілеспрямованих і випадкових загроз та мандатною політикою безпеки.

Рис. 3. Функціональна структура геоінформаційної системи

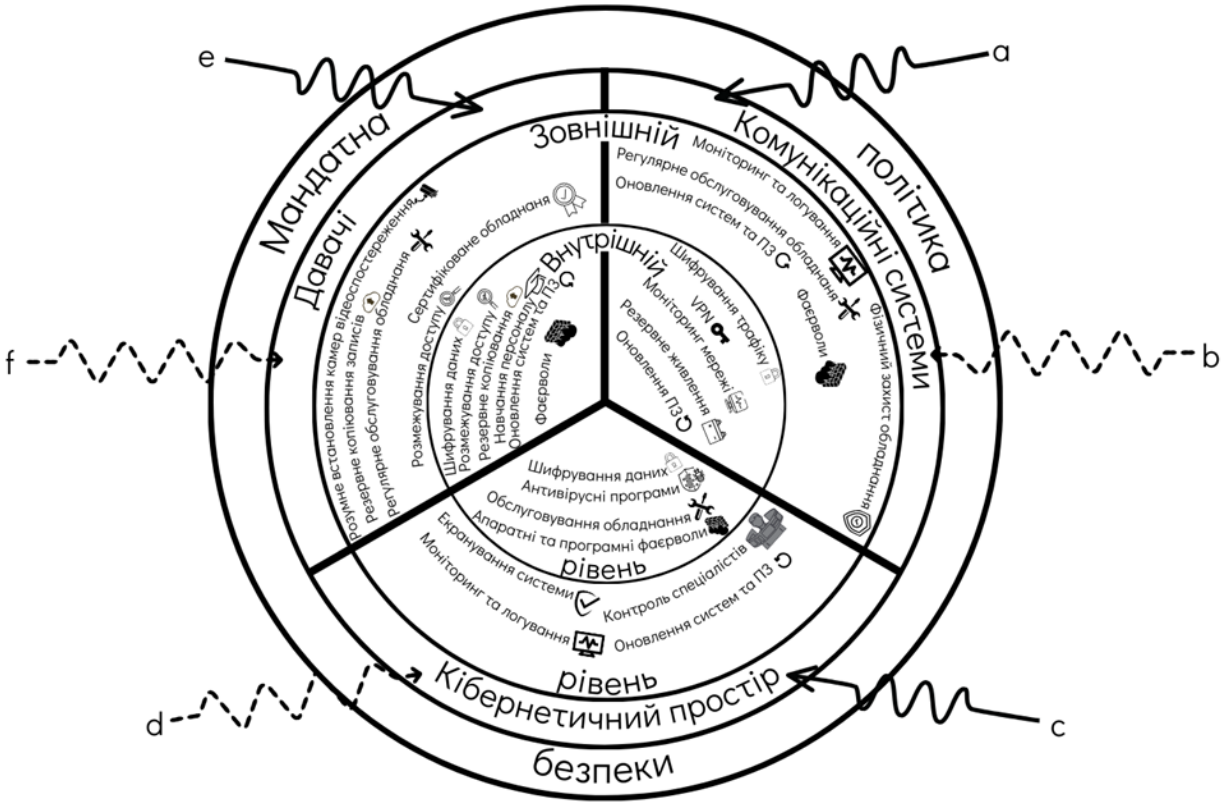

Рис. 4. Інтегральна модель безпеки ІКФС моніторингу надзвичайних ситуацій екосистеми регіону: a, c, e – цілеспрямовані загрози; b, d, f – випадкові загрози

Комплексні системи безпеки багаторівневої ІКФС. Комплексні системи безпеки багаторівневої ІКФС моніторингу надзвичайних ситуацій на зовнішньому і внутрішньому рівнях безпеки наведені відповідно в таблицях 2 і 3.

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

Таблиця 2

КСБ багаторівневої ІКФС на зовнішньому рівні

Рівень ІКФС	**Цілеспрямовані загрози**	**Випадкові загрози**	**Технології безпеки**
Фізичний простір: давачі відбору даних	Злам системи керування давачами для надання хибних даних Введення шкідливого ПЗ у систему моніторингу, що призводить до перехоплення/зміни даних. DoS/DDoS атаки на систему моніторингу	Зупинка обміну даними через злам Злам давача через неправильне його встановлення Негативний вплив погодних умов	Використання сертифікованого обладнання Розмежування доступу до приміщень/території/окремих систем моніторингу Регулярні перевірки та обслуговування давачів
Фізичний простір: давачі безпеки (системи відеоспостереження)	Перехоплення відеосигналу між камерами та системою запису, що дозволяє зловмисникам переглядати відео без авторизації Перевантаження системи відеоспостереження через масовий запит на доступ до відеопотоку/ресурсів може призвести до переривання нормального функціонування.	Відмова вузлів системи відео-спостереження Зупинка систем із-за відсутності живлення Пошкодження/втрата файлів через неправильну конфігурацію системи відео-спостереження	Регулярні перевірки програмного забезпечення камер та комп'ютерів, що ними керують Встановлення камер відеоспостереження з можливим перехресним спостереженням Встановлення камер відеоспостереження в важкодоступних місцях Резервне копіювання записів з камер
Комунікаційне середовище: LoRaWAN	Перехоплення даних між пристроєм та шлюзом, що призводить до зміни/підроблення переданих повідомлень Можливе перехоплення конфіденційних даних, наприклад параметрів давачів/даних про об'єкт моніторингу Атака на шлюзи може перевантажити мережу, що призведить до відмови в обслуговуванні та недоступності пристроїв Навмисна неавторизована зміна пакетів даних може призвести до передавання хибної інформації на сервер/некоректного управління пристроями. Злам ключів безпеки та під'єднання підробленого пристрою до мережі для викрадення даних	Пристрої, що працюють на тих самих частотах, створюють перешкоди Перепади напруги/розряджання батарей, пристрої можуть унеможливити з'єднання Природні/ фізичні перешкоди можуть погіршувати якість передавання сигналу між пристроями та шлюзами Зношування/збої у функціонуванні компонентів спричинюють нестабільність зв'язку	Використання AES-128 для шифрування як на рівні мережі/ додатків забезпечує захист від перехоплення та підроблення даних Передавання даних здійснюється лише після аутентифікації пристрою та сервера, що знижує ризик під'єднання підроблених пристроїв Використання пристроями LoRaWAN окремих ключів (NwkSKey та AppSKey) для мережевої та прикладної частин мінімізує ризики компрометації Забезпечення цілісності повідомлень за допомогою MIC (Message Integrity Code) гарантує коректність переданих даних Використання частотного розподілу з метою уникнення перешкод та впливу випадкових сигналів
Комунікаційне середовище: GPS	Маніпулювання GPS-сигналами для передавання хибної інформації щодо місця перебування	Переривання зв'язку через зміну умов передавання даних (зміну	Залучення кваліфікованих працівників, логування та перевірки їх дій з метою

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

	Перешкоджання роботі GPS -приймачів шляхом імітації GPS-сигналів Використання підроблених GPS-сигналів з метою впливу на поведінку користувачів	швидкості передавання даних/затримки) Погіршення точності через перешкоди у мережевому середовищі	мінімізації небезпеки людського фактору Своєчасне оновлення програмного забезпечення, використання сучасних протоколів передавання та захисту мінімізує ризики втрати/підроблення GPS-сигналу
Комунікаційне середовище: LTE	DoS/DDoS атаки на мережу LTE Використання вразливостей реалізації LTE-протоколів Фішингові атаки на абонентів LTE-мереж Пошкодження обладнання базової станції LTE Фізичне перешкоджання сигналу LTE	Неякісна конфігурація систем через суб'єктивні помилки Погана якість зв'язку через погодні умови Пошкодження мережевих пристроїв	Використання фаєрволів/фільтрування для захисту від мережевих розподілених атак Регулярні перевірки обладнання, встановлення обладнання у важкодоступних місцях Фізичний захист від викрадення та погодних умов
Кібернетичний простір: геоінформа-ційна система	Атаки, спрямовані на підроблення, зміну/видалення просторових даних для спотворення інформації, що призводить до хибних управлінських рішень Атаки для отримання доступу до облікових записів операторів ГІС, що відкривають зловмисникам можливість втручатися у функціонування системи/ отримання доступу до конфіденційних даних Перевантаження мережевих/обчислювальних ресурсів, що призводить до збоїв у роботі системи Ін'єкція шкідливих модулів/оновлень у систему, що призводить до порушення її функціональності	Суб'єктивні помилки можуть призвести до спотворення інформації, збоїв у системі та хибного реагування Несвоєчасне оновлення ПЗ може залишити систему вразливою до загроз/викликати несумісність з новими компонентами Велика кількість запитів на обробку даних через різке підвищення активності (наприклад, під час стихійного лиха) може перевантажити систему та знизити її продуктивність.	Поділ мережі ГІС на ізольовані сегменти мінімізує ризики поширення загроз між підсистемами Використання двофакторної/багатофакторної аутентифікації операторами ГІС обмежує доступ до лише авторизованих користувачів. Шифрування просторових даних під час передавання та зберігання захищає їх від несанкціонованого доступу, запобігаючи їх витоку/зміні. Регулярні оновлення захисту від відомих вразливостей знижують ризик атак на ГІС Резервне копіювання просторових даних забезпечує відновлення інформації у разі втрати/пошкодження в результаті випадкових збоїв/атак.

Таблиця 3

КСБ багаторівневої ІКФС на внутрішньому рівні

Рівень ІКФС	**Цілеспрямовані загрози**	**Випадкові загрози**	**Технології безпеки**
Фізичний простір: пристрої Інтернету речей	Несанкціонований доступ до моніторингових даних з давачів	Нестабільна напруга/ від'єднання енергозабезпечення	Шифрування даних від несанкціонованого доступу Регулярне оновлення програмного забезпечення

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

	Виникнення вразливостей у програмному та апаратному забезпеченні давачів	призводять до збоїв пристроїв Випадкові перешкоди від інших пристроїв можуть погіршити якість ввідбору даних	Захист апаратного забезпечення від несанкціонованих змін Застосування цифрових підписів для підтвердження автентичності результатів
Комунікаційне середовище: безпровідні мережі	Атаки, спрямовані на перевантаження мережевого обладнання за допомогою великої кількості запитів з різних джерел, що може призвести до відмови в обслуговуванні Шкідливе програмне забезпечення, що розповсюджується через мережу, може заражати мережеве обладнання, використовуючи його для розповсюдження	Випадкові перепади напруги можуть пошкодити обладнання мережі, та його відмову Недостатня вентиляція або неправильна експлуатація може призвести до перегріву мережевого обладнання та відмови або пошкодження.	Віртуальні приватні мережі (VPN) Шифрування трафіку Оновлення програмного забезпечення Створення бекапів конфігурацій Розмежування доступу Моніторинг мережевої активності Технології безпеки безпровідних мереж Хмарні рішення безпеки Резервне живлення та резервування
Кібернетичний простір: бази даних	Цілеспрямовані порушення конфіденційності Атаки з метою відмови сервісу для користувачів Отримання несанкціонованого віддаленого доступу	Випадкове видалення, помилкові внесення, пошкодження даних Переповнення бази даних Конфлікти паралельних транзакцій	Шифрування бази даних Регулярне оновлення ПЗ Аудит безпеки Регулярне резервне копіювання Розмежування доступу Механізми аутентифікації Навчання персоналу
Кібернетичний простір: термінали користувачів	Розподілена атака перебору паролів (Brute Force Attack). Атака з відмовою в обслуговуванні (Denial-of-Service, DoS). Використання вразливостей ПЗ Розповсюдження шкідливого ПЗ Використання шкідливого поштового вмісту	Випадкове під’єднання до небезпечних мереж Випадкові вразливості ПЗ Неправильне налаштування приватності Недбалість у зберіганні паролів Неправильне використання облікового запису	Використання антивірусного програмного забезпечення. Використання фаєрволів Регулярні оновлення ПЗ Використання паролів і парольних менеджерів Використання бекапів даних Навчання у сфері мережевої безпеки Використання технологій захисту від фішингу Обмеження прав адміністратора

Мандатна політика безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Для ІКФС моніторингу надзвичайних ситуацій екосистеми регіону розглянемо узагальнену модель мандатної (багаторівневої) політики безпеки (рис. 5).

Мандатна політика безпеки має перевагою, у порівнянні з дискреційною та рольовою політиками, високий ступінь надійності захисту. Мандатна політика безпеки ІКФС моніторингу надзвичайних ситуацій, яка грунтується на мандатному керуванні доступом, охоплює вимоги: 1) визначеність решітки конфіденційності інформації; надання кожному об'єктові системи відповідного рівня конфіденційності за ступенем цінності інформації

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

відносно об’єкта; 2) задоволення вимог ідентифікації всіх суб'єктів та об'єктів системи; 3) реалізація алгоритму запобігання витоку інформації між об’єктами з різними рівнями доступу.

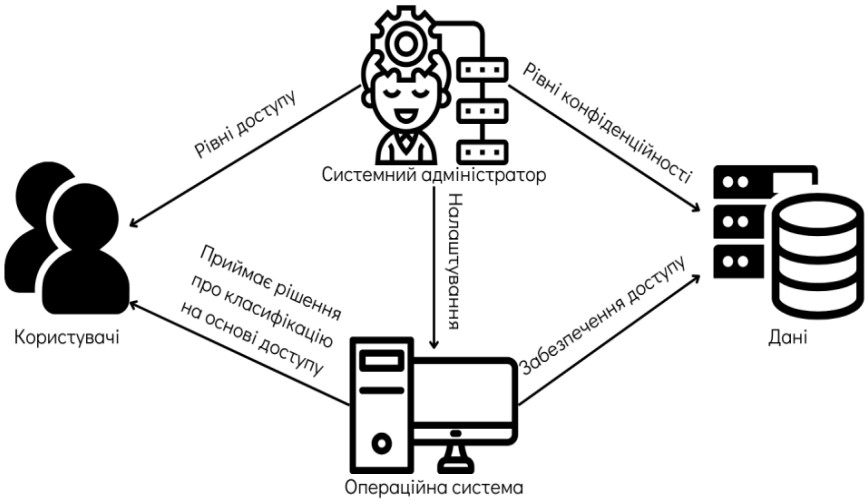

Рис. 5. Модель мандатної політики безпеки ІКФС

Обов’язковий контроль доступу забезпечує дотримання набору правил безпеки, які регламентують доступ користувачів/систем до певних ресурсів. Мандатна політика безпеки ІКФС уможливлює: оцінювання загроз і ризиків на рівні проведення ідентифікації уразливостей; впровадження політики доступу та аутентифікації на рівні встановлення визначених правил, а також механізмів аутентифікації користувачів; захист даних на рівні розроблення стратегій безпеки конфіденційної інформації засобами шифрування; навчання персоналу на рівні проведення відповідних тренінгів; моніторинг та реагування на інциденти на рівні реалізації систем відслідковування подій в системі.

Висновки

В роботі запропоновано методологічні засади безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій впливу факторів техногенного і природного характеру на основі універсальної платформи, яка охоплює: 1) архітектуру багаторівневої ІКФС “давачі – безпровідне комунікаційне середовище – геоінформаційна система”; 2) інтегральну модель багаторівневої безпеки ІКФС; 3) комплексну систему безпеки ІКФС згідно з концепцією “об’єкт – загроза – захист”, 4) мандатну політику безпеки ІКФС, що є розвитком системних підходів до безпечного моніторингу надзвичайних ситуацій регіону в умовах глобальних викликів суспільства.

Перелік посилань

1.Стратегія кібербезпеки України. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#n12.

2.Kozhedub, Y.V., Kramska, Y.A., & Gyrda, V.A. (2020). Analysis of human factor influence on cyber-physical system. Information Technology and Security, 8(1), 102-115.

3.Meytus, V., Morozova, G., Taran, L., Kozlova, V., & Maidaniuk, N. (2019). Cyber-physical systems as a basis for intellectualization of smart enterprises. Control Systems and Computers, 4(282), 14-26.

4.Mutua, E. (2024). Cyber-Physical Systems and Their Role in Industry 4.0. Journal of Technology and Systems, 6(5), 57-69. doi: 10.47941/jts.2149.

5.Ahmad, Z., Islam, U., & Riaz, S. (2024). Complexity Analysis of Industrial Scale Cyber Physical Systems. In 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS) (pp. 1-6). St. Louis, MO: IEEE.

6.Pogasiy, S.S. (2022). Models and methods of information protection in cyber-physical systems. Information Security, 28(2), 67-79.

© Дудикевич В.Б., Микитин Г.В., Бордуляк С.М., Фур Я.М. (2025). Комплексна система безпеки інтелектуальної кіберфізичної системи моніторингу надзвичайних ситуацій. Сучасний захист інформації, 1(61), 249–258. https://doi.org/10.31673/2409-7292.2025.014428.

7.Шологон О.З. (2015). Безпека у кіберфізичних системах. Кіберфізичні системи досягнення та виклики: матеріали першого Наукового семінару (с. 132-137). Львів: Національний університет “Львівська політехніка”: НВФ “Українські технології”.

8.Furrer, F.J. (2023). Safe and secure system architectures for cyber-physical systems. Informatik Spektrum, 46, 96–103. doi: 10.1007/s00287-023-01533-z.

9.Бобало Ю.Я., Дудикевич В.Б., & Микитин Г.В. (2020). Стратегічна безпека системи “об’єкт – інформаційна технологія”. Львів: Видавництво НУ “Львівська політехніка”.

10.Yang, T., Liu, Y., & Li, W. (2022). Attack and defence methods in cyber-physical power system. IET Energy Systems Integration, 4(2), 159-170.

11.Mittal, S., Tolk, A., Haque, M.A., Shetty, S., & Krishnappa, B. (2019). Cyber-physical system resilience. In S. Mittal & A. Tolk (Eds.), Complexity Challenges in Cyber-Physical Systems (pp. 301-337). John Wiley & Sons.

12.Nakirya, J.B. (2024). Cyber-Physical Systems: Integrating Computing with Physical Processes. Research Output Journal of Engineering and Scientific Research, 3(2), 49-52.

13.Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H.H. (2023). A survey on cyber–physical systems security. IEEE Internet of Things Journal, 10(24), 21670-21686.

14.Regulations on the interaction of subjects of monitoring, surveillance, laboratory control and forecasting of emergencies. (2018). Retrieved from https://dsns.gov.ua/upload/1/2/6/3/6/2018-2-24-reglament-monatoring.odt?__cf_chl_tk=uRf577YiOBdD_eQFmtxeelDKT_B_CpY.32UWrSL5jms-1730019053-1.0.1.1-4Vno.OAFXRREH35LgX87pC5lrbKs4SH_cH83ncCtsPI.

15.Zatserkovnyi, V.I., Burachek, V.G., Zheleznyak, O.O., & Tereshchenko, A.O. (2014). Geoinformation systems and databases: monograph. Nizhyn: Nizhyn State University named after M. Gogolya.

Надійшла 23.02.2025