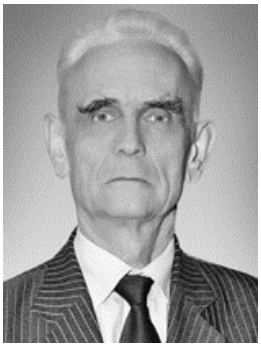
© Dudykevych V., Mykytyn G., Sydoryk D. Building a Comprehensive Multi-Level Security Model for the Cyber-Physical Intelligent Transport System// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 100-109. ©

DOI: 10.18372/2225-5036.30.18611

ПОБУДОВА КОМПЛЕКСНОЇ БАГАТОРІВНЕВОЇ МОДЕЛІ БЕЗПЕКИ КІБЕРФІЗИЧНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТРАНСПОРТНОЇ СИСТЕМИ

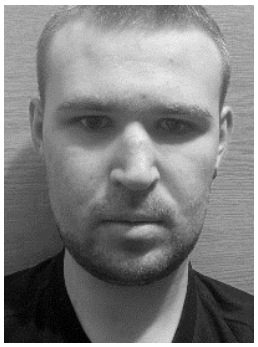
Валерій Дудикевич, Галина Микитин, Дмитро Сидорик

Національний університет "Львівська політехніка"



ДУДИКЕВИЧ Валерій Богданович, д.т.н., професор, заслужений винахідник України
Рік та місце народження: 1941 рік, с. Біло-Скелюватe Ново-Світлівського району Луганської обл.,Україна.
Освіта: Львівський політехнічний інститут, 1963 рік.
Посада: професор кафедри захисту інформації, керівник Західного регіонального навчально-наукового центру захисту інформації.
Наукові інтереси: інформаційна безпека, технічний захист інформації, число-імпульсні перетворювачі кодів для вимірювання і управління.
Публікації: понад 600 наукових публікацій, серед яких біля 200 винаходів, монографії, наукові статті , підручники та навчально -методичні посібники.
E-mail: vdudykev@gmail.com.
Orcid ID: 0000-0001-8827-9920.

МИКИТИН Галина Василівна, д.т.н., професор
Рік та місце народження: 1962 рік, м. Тлумач Івано-Франківської області, Україна.
Освіта: Львівський політехнічний інститут, 1986 рік.
Посада: професор кафедри захисту інформації.
Наукові інтереси: безпека інформаційно-комунікаційних технологій; безпека кіберфізичних систем; безпека технологій процесів інтелектуалізації.
Публікації: більше 300 наукових публікацій, серед яких наукові статті, монографії, довідник та навчально-методичні посібники.
E-mail: cosmos-zirka@ukr.net.
Orcid ID: 0000-0003-4275-8285.



СИДОРИК Дмитро Олегович, магістрант
Рік та місце народження: 2001 рік, м. Вінниця, Україна.
Освіта: магістрант кафедри захисту інформації Національного університету "Львівська політехніка", 2023 рік.
Посада: магістрант кафедри захисту інформації Національного університету «Львівська політехніка».
Наукові інтереси: безпека комп'ютерних мереж, безпека кіберфізичних систем.
Публікації: тези Всеукраїнської науково-практичної конференції.
E-mail: dimsydr@gmail.com.
Orcid ID: 0009-0005-2233-8867.

Анотація. *Розглянуто узагальнену архітектуру інтелектуальної транспортної системи (ІТС) на основі багаторівневої кіберфізичної системи (КФС): давачі фізичного простору, безпровідні технології комунікаційного середовища, автоматизована система обробки інформації (АСОІ) кібернетичного простору. Запропоновано комплексну модель безпеки ІТС у просторі "багаторівнева КФС – багаторівнева безпека". Побудовано комплексні системи безпеки (КСБ): фізичного і кібернетичного просторів кіберфізичної ІТС на основі моделі загроз STRIDE – на зовнішньому рівні; комунікаційного середовища на основі мережевої моделі OSI – на внутрішньому рівні. Розроблено програмну реалізацію симетричного блокового шифрування повідомлень на основі алгоритму "Калина" засобами мови програмування C# в комунікаційному середовищі ІТС.*

Ключові слова*: інтелектуальний транспорт, кіберфізична система, фізичний простір, комунікаційне середовище, кібернетичний простір, багаторівнева комплексна модель безпеки, комплексна система безпеки, загрози, технології безпеки, алгоритм шифрування повідомлень.*

Постановка проблеми

Розгортання Концепції Індустрія 4.0 в Україні в різних сегментах інфраструктури суспільства має одним з основних векторів – створення нових підходів до забезпечення безпеки інформаційних та комунікаційних технологій підтримки функціонування інтелектуальних об'єктів [1, 2, 3, 4, 5]. Концепція безпечного "Розумного міста" є центральною в просторі процесів інтелектуалізації і передбачає комплекс предметно-орієнтованих сегментів інфраструктури міста – освіту, екологію, енергетику, медицину, транспорт т.і. [6].

Одним із ефективних основних інструментаріїв підтримки безпечного функціонування сегментів "Розумного міста" є кіберфізичні системи [7]. Відповідно постає проблема безпеки КФС, зокрема у частині безпечного інтелектуального транспорту.

Аналіз останніх досліджень і публікацій

Сьогодні актуальним є розвиток методологічних підходів і інформаційно-комунікаційних технологій підтримки функціонування інтелектуального транспорту. Питання забезпечення безпечних і надійних технологій зв'язку в сегментах "Розумного міста" на рівні пристроїв Інтернету речей проаналізовано в праці [8]. Цікавим є комплексний підхід до забезпечення контролю доступу і безпеки інтелектуального автомобільного транспорту, що ґрунтується на автентифікації транспортних засобів у безпровідній мережі VANET та ідентифікації різноманітних кібератак і відповідно реалізується на рівні шифрування і методів глибокого навчання [9]. В праці [10] проведено аналіз безпеки автономних транспортних систем, наприклад безпілотних літальних апаратів з урахуванням кібератак і підходу до захисту на основі технологій штучного інтелекту. У просторі безпечної інтелектуалізації транспорту досліджуються: елементи впровадження КФС для функціонування ІТС [11]; аспекти безпеки КФС у додатках Smart City [12]; оцінювання ризиків для транспортної інфраструктури на основі кіберфізичної системи [13].

Мета та постановка завдання

В роботі пропонується розглянути: побудову багаторівневої комплексної моделі безпеки кіберфізичної ІТС і, на цій основі, створення комплексних систем безпеки багаторівневої КФС в просторі "загрози – захист"; розроблення програмного забезпечення шифрування повідомлень на основі алгоритму "Калина" засобами мови C#. Розвиток методологічних підходів до безпеки кіберфізичних систем забезпечить ефективне безпечне функціонування інтелектуальної транспортної системи.

Виклад основного матеріалу дослідження

Архітектура багаторівневої кіберфізичної інтелектуальної транспортної системи. На рисунку представлена узагальнена архітектура інтелектуального транспорту на основі багаторівневої кіберфізичної системи (рис. 1). Фізичний простір кіберфізичної ІТС функціонує на основі давачів: контролю безпеки в просторі відеоспостереження; контролю параметрів ІТС – оплати за проїзд (валідатор безконтактних карток), функціоналу дверей; параметрів комфортності салону – температури (кондиціонер), даних про маршрут (інформаційне табло), маршрут (аудіо-інформатор).

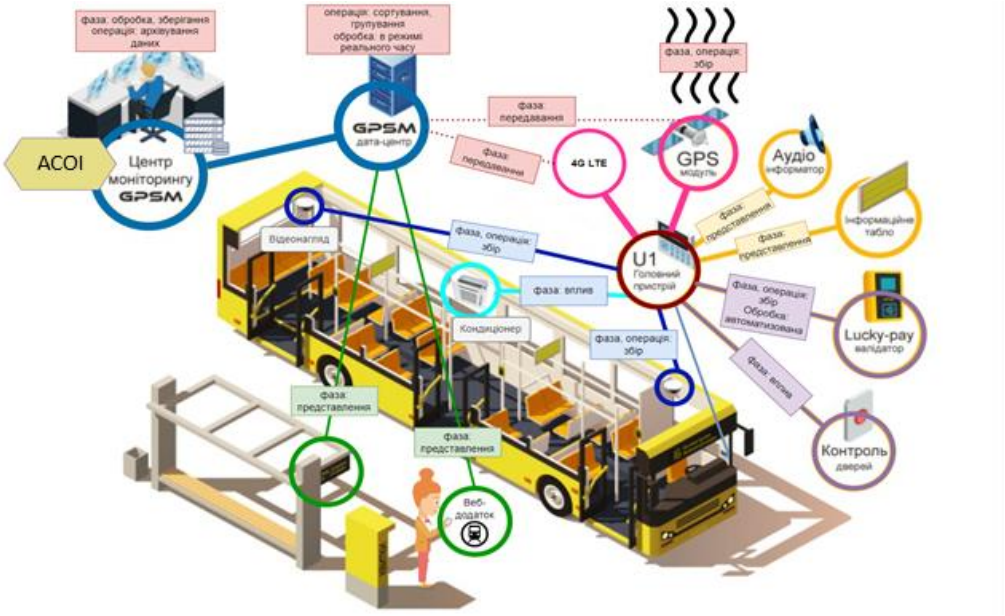


Рис. 1. Архітектура безпечного інтелектуального транспорту на основі кіберфізичної системи

Комунікаційне середовище ІТС функціонує на основі: безпровідної технології LTE (Long-Term Evolution) і технології відстеження GPS (Global Positioning System). LTE – стандарт безпровідної технології обміну даними у мобільних мережах, що забезпечує високу швидкість і надійне з'єднання для мобільних пристроїв. Функціональні параметри стандарту LTE: частотний діапазон – 700 МГц – 2600 МГц; швидкість передавання даних – до 1 Гбіт/с; дальність зв'язку – до 10 км. Основні компоненти архітектури LTE (рис. 2): eNodeB – базова станція для безпровідного з'єднання з мобільними пристроями; MME – вузол управління мобільністю, керує мобільними станціями та переміщенням мобільних пристроїв UE в мережі LTE; UE – мобільний пристрій, що підключається до мережі LTE; E-UTRAN – безпровідна частина мережі LTE, включаючи eNodeB та радіоінтерфейс. GPS – технологія визначення місцезнаходження та навігації,

використовує сигнали з супутників GPS для точного визначення координат (рис. 2).

Функціональні параметри GPS-технології: частотний діапазон – 1176.45 МГц – 1575.42 МГц; швидкість передавання даних – 50 біт/с (початкова); мінімум супутників – 4; швидкість локації – декілька секунд – декілька хвилин.

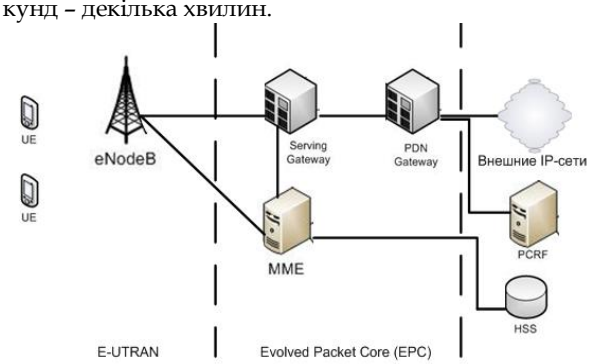


Рис. 2. Архітектура технології LTE

Основні компоненти архітектура GPS (Global Positioning System (рис. 3): UE (User Equipment): приймач GPS, який може бути вбудованим у мобільні пристрої; GPS Satellites: супутники, розташовані у космосі, які передають сигнали GPS, надають інформацію про своє розташування і точний час; Base Station – наземна станція, яка приймає сигнали від GPS супутників та надає їх UE для обробки; MSC (Mobile Switching Center) – центральний елемент мобільної мережі, який виконує керування даними та комутацію між UE та іншими мережевими елементами; AGPS (Assisted GPS) Receiver – пристрій або функціональність в UE, яка використовує додаткову інформацію для поліпшення продуктивності та швидкості отримання сигналу GPS.

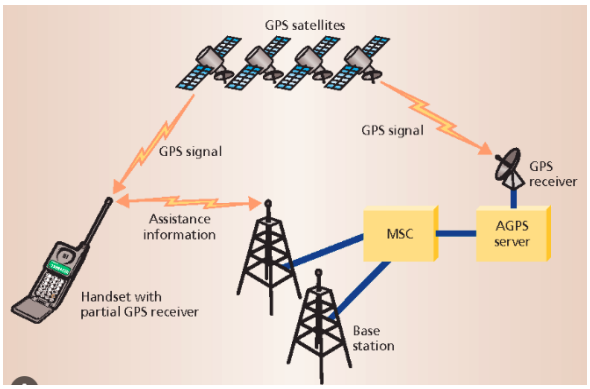


Рис. 3. Архітектура GPS-технології

Кібернетичний простір представлений: інформаційними ресурсами (ІР), інформаційною системою (ІС), інформаційними процесами (ІП), що дозволяє аналізувати поведінку системи та приймати стратегічні рішення в рамках оптимізації т.і. Інформаційні ресурси – бази даних, сховища даних. Бази даних – впорядкований набір взаємопов'язаних даних: дані про наявний транспорт, його характеристики, дані про персонал, дані про зареєстрованих клієнтів. Сховища даних – певним чином агреговані дані, наприклад статистичні дані про час проходження певних маршрутів, середня окупність маршруту, витрата палива, час максимального та мінімального пасажиропотоків. Інформаційна система – автоматизована система обробки інформації (АСОІ), в якій сукупність всіх операцій реалізується програмно-технічними засобами з метою передавання інформації на запит користувача. В АСОІ надходить інформація з GPSM – програмно-апаратного комплексу моніторингу GPS-пристроїв. Інформаційні процеси: фаза, операція, обробка. Фаза – представляє етап ІП: збір, передавання, обробка, зберігання, представлення. Операція – характеризує функцію, що виконується під час ІП: збір, сортування, групування, архівування даних. Обробка – характеризує яким чином дані обробляються під час ІП: автоматизовано, в режимі реального часу.

Комплексна багаторівнева модель безпеки кіберфізичної інтелектуальної транспортної системи

На рисунку представлена комплексна багаторівнева модель безпеки кіберфізичної інтелектуальної транспортної системи (рис. 4). Зовнішній рівень моделі безпеки багаторівневої кіберфізичної ІТС побудований в просторі "загрози – захист", що передбачає:

1) модель загроз STRIDE – для фізичного простору; мережеву модель OSI (базову еталонну модель взаємодії відкритих систем), зокрема її фізичний (1), канальний (2) і мережевий (3) рівні – для комунікаційного середовища ІТС; модель загроз основним профілям безпеки – конфіденційності (К), цілісності (Ц), доступності (Д) – для кібернетичного простору;

2) технології безпеки відповідно до рівнів ІТС та ймовірних загроз.

Внутрішній рівень моделі безпеки відповідно передбачає:

1) модель загроз STRIDE – для фізичного і кібернетичного просторів; модель відкритих систем OSI для 1, 2, 3 рівнів комунікаційного середовища ІТС;

2) технології безпеки відповідно до рівнів ІТС та ймовірних загроз. Мандатна політика безпеки – це політика, що ґрунтується на класифікації інформації за її рівнем захищеності та наданні доступу до неї суб'єкту за рівнем допуску, який прописаний у його мандаті. Основним завданням мандатної політики безпеки є захист інформації з високим рівнем доступу від користувачів з нижчим рівнем, що дозволяє запобігти витоку інформації через людський фактор.

Комплексна система безпеки фізичного простору і комунікаційного середовища ІТС: зовнішній рівень

КСБ фізичного простору ІТС: модель загроз STRIDE. В таблиці представлений зовнішній рівень КСБ кіберфізичної ІТС на основі моделі загроз STRIDE: загроза підробки (Spoofing/автентичність) – зловмисник проникає в систему з підробленим ідентифікатором, тим самим надаючи собі доступ до конфіденційної інформації; загроза зміни даних (Tampering/ цілісність) – зловмисник змінює або видаляє дані, що може призвести до порушення цілісності та доступності системи; відмова від авторства (Repudiation/ авторство) – користувачі можуть заперечувати заходи безпеки, які вони виконували, такі як вхід або зміни в системі; загроза розголошення інформації (Information Disclosure/ конфіденційність) – зловмисник намагається отримати конфіденційну інформацію, що може спричинити нанесення шкоди системі та її користувачам; зловмисник забезпечує неможливість доступу до ресурсів системи, що може призвести до зупинки її роботи; загроза відмови в обслуговуванні (Denial of Service/ доступність) – зловмисник

забезпечує неможливість доступу до ресурсів системи, що може призвести до зупинки її роботи; загроза зламу (Elevation of Privilege/ авторизація) – зловмисник збільшує рівень привілеїв в системі, що дає йому більше можливостей для зловживання (табл. 1).

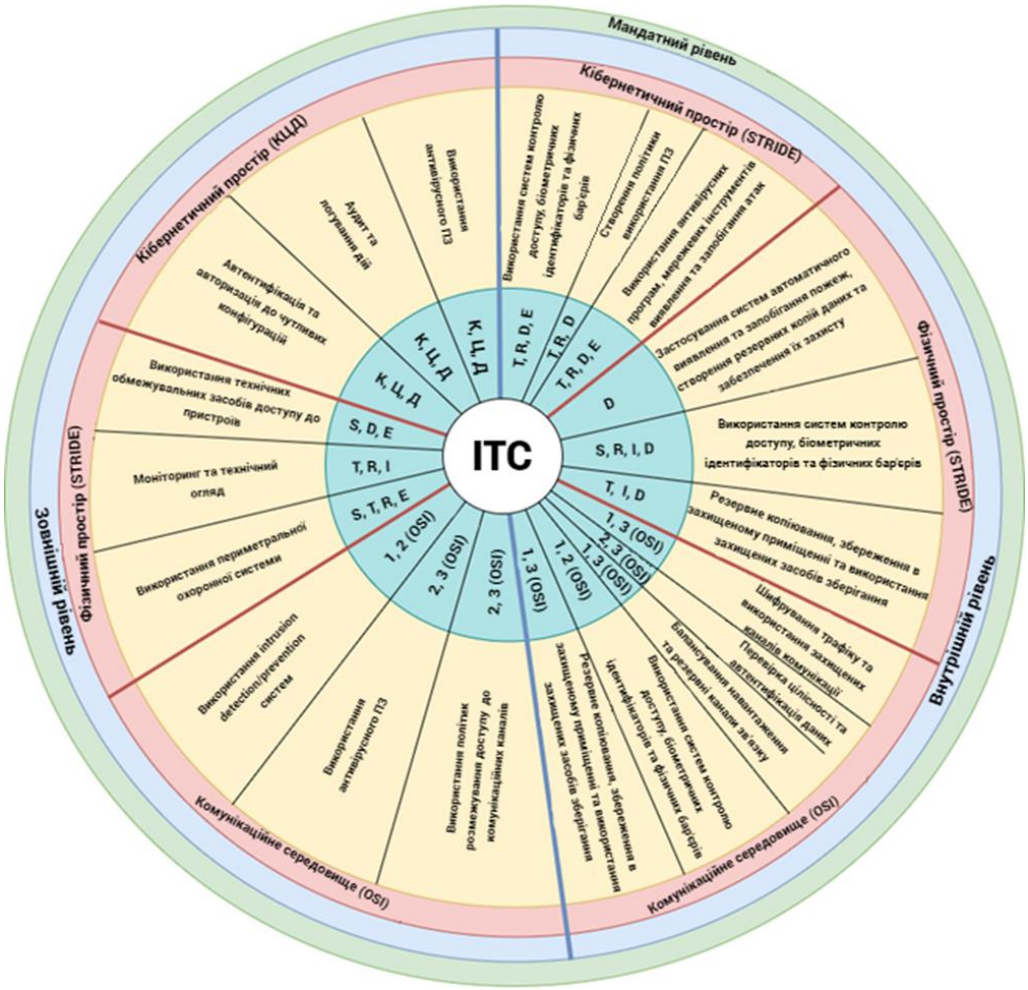


Рис. 4. Комплексна багаторівнева модель безпеки кіберфізичної ІТС: загрози – захист

КСБ комунікаційного середовища ІТС: модель OSI

Для побудови комплексної системи безпеки проаналізуємо ймовірні загрози на фізичному (1), канальному (2), мережевому (3) рівнях моделі OSI. На рівні (1) проявляються загрози фізичного пошкодження кабелів/ обладнання, віруси на фізичних носіях інформації т.і. На рівні (2) проявляються атаки на протоколи мережевого доступу, підробка MAC-адрес, атаки на стійкість до перенаправлення т. і. На рівні (3) проявляються атаки на протоколи мережевого рішення, флуд, DNS-атаки т. і.

КСБ кібернетичного простору кіберфізичної ІТС: внутрішній рівень.

КСБ автоматизованої системи обробки даних кібернетичного простору ІТС. Представлена комплексна система безпеки АСОІ на основі моделі загроз STRIDE (табл. 3). КСБ інформаційних процесів кібернетичного простору кіберфізичної ІТС на рівні: фази, операцій, обробки: в табл. 4, 5, 6 відповідно представлені комплексні системи безпеки ІП на етапах – фази, операцій, обробки за впливу ймовірних загроз на апаратно-програмний рівень кіберфізичної ІТС.

Захищений канал комунікаційного середовища ІТС: програмна реалізація шифрування даних на основі алгоритму "Калина" та мови програмування C#: особливостями блокового симетричного алгоритму шифрування "Калина" (ДСТУ 7624: 2014) є максимальний рівень криптостійкості, зокрема для розміру блоку і довжини ключа 512/512 біт та відповідно висока швидкодія перетворень 1386.46 Мбіт/с. Для програмної реалізації алгоритму "Калина" використана мова програмування C#, швидкодія та кросплатформеність якої дозволить використовувати програму на будь-якому пристрої для захисту інформації в технологіях безпровідного зв'язку. На рис. 5, 6 наведені блок-схеми програмної реалізації шифрування даних та відповідно генерації раундових ключів.

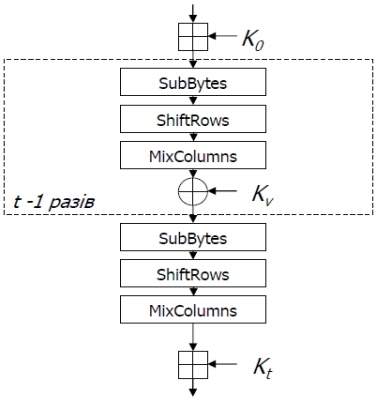


Рис. 5. Блок-схема шифрування даних

Таблиця 1

КСБ фізичного простору кіберфізичної ІТС на основі STRIDE : випадкові і цілеспрямовані загрози

Давачі	Модель STRIDE	Загрози		Технології безпеки
		Випадкові	Систематичні	
Системи відеоспостереження та контроль оплати	**S**TRIDE автентичність	Стихійне лихо; людський фактор; втрата живлення; втрата мережі LTE.	NFC Skimming; DeepFake-модифікація саботаж вразливе та вірусне ПЗ; втручання хакерів в систему.	Забезпечення кількох джерел живлення; встановлення надійного IDS для виявлення вторгнень та втручань в ПЗ об'єкта; лекції з безпеки для працівників та регулярний огляд системи оплати відповідальною особою; стійкий алгоритм шифрування транзакцій, відео; ведення журналу подій для подальшого аналізу.
Давач звукового супроводу маршруту	S**T**RIDE цілісність	Людський фактор; відмова або випадкове спрацювання.	Віддалений спосіб атаки для відтворення певної аудіодоріжки; вразливе та вірусне ПЗ; саботаж; несумісність з іншими системами після оновлення.	Своєчасне оновлення системи та регулярна перевірка сумісності; встановлення надійного IDS для виявлення; ведення журналу подій для подальшого аналізу; фізична перевірка справності давача.
Системи відеоспостереження, інфо-табло, давач звукового супроводу маршруту	ST**R**IDE авторство	Відмова давача через несправність або брак; стихійне лихо; людський фактор.	Обхід зловмисником системи та вивід фейкових даних на табло; DeepFake-модифікація; саботаж.	Резервне копіювання даних на віддалений сервер; ведення журналу подій для подальшого аналізу; архівування та шифрування даних відеокамери для відправлення та аналізу в хмарному середовищі; надсилання конкретних відрізків відео на віддалений сервер під час виникнення аномалій; використання нейромережевих технологій на базі методів машинного навчання з метою онлайн-аналізу відео; надійне шифрування трафіку, щоб уникнути перехоплення та модифікації даних на інформаційній таблиці.
Системи відеоспостереження та контроль оплати	STR**I**DE (конфіденцій-ність)	Стихійне лихо; людський фактор; відмова систем живлення; збої чи нестабільність роботи технічних пристроїв.	Віддалене внесення змін до програмного забезпечення давачів та їх деактивація; віддалений взлом контролю оплати; саботаж; віруси, піратське ПЗ.	Забезпечення пристроїв декількома джерелами живлення; Реалізація програмного комплексу, що зберігатиме в журналі подій будь-яку санкціоновану та несанкціоновану дію користувача, а також валідуватиме дані, які ввів користувач під час конфігурації давачів; надійне асиметричне шифрування RSA-4096; додатковий фізичний захист давачів; своєчасне оновлення системи, антивірусного ПЗ, IDS; систематичний огляд давачів спеціалістами.
Інфо-табло, GPS-трекер, кондиціонер	STRI**D**E (доступність)	Стихійне лихо; людський фактор; затримка в передаванні даних через проблеми з мережею; відмова давача через несправність.	Віддалене вимкнення GPS-трекеру, інформаційної таблиці; підроблення повідомлень таблиці; відключення GPS працівником.	Забезпечення декількох джерел живлення; використання машинного навчання, для аналізу переміщень в реальному часі; фізичний захист трекера; ведення журналу подій для подальшого аналізу; надійне шифрування трафіку, щоб уникнути перехоплення та модифікації даних на інформаційній таблиці; мережевий брандмауер для блокування шкідливих вхідних пакетів; антивірус та IDS.
Контроль оплати	STRID**E** (авторизація)	Відмова чи збої роботи давача; пошкодження давача; стихійне лихо; людський фактор.	Сканування транзакцій; взлом алгоритмів безпеки; підроблення сигналу.	Використання IDS з алгоритмами машинного навчання для виявлення вторгнень; захист від пошкоджень давача та виявлення зчитувачів; систематична перевірка терміналу спеціалістом; багатофакторна авторизація.

Таблиця 2

КСБ безпровідних технологій LTE, GPS кіберфізичної ІТС на основі OSI: випадкові і цілеспрямовані загрози

Технологія	Рівень мережевої моделі OSI	Загрози		Технології безпеки
		Випадкові	Систематичні	
LTE	Фізичний	Електромагнітні перешкоди; Спотворення сигналу; Перешкоди на маршруті сигналу; Втрати енергії сигналу; Міжсимвольна та міжкадрова інтерференції; Синхронізація помилок.	Атаки на базові станції: злам або компроментація базових станцій; Забруднення спектра шляхом випромінювання небажаних сигналів або перешкод на частотах, використовуваних мережею LTE; Атаки на канали зв'язку; Перехоплення даних за допомогою техніки аналізу трафіку.	Вбудовані алгоритми шифрування AES, AKA; Аутентифікація; Контроль доступу до обладнання; Використання захищених приміщень; Використання систем моніторингу та виявлення вторгнень (IDS/IPS); Фізичне шифрування з'єднань.
LTE	Канальний	Розсіювання сигналу; Вплив сторонніх сигналів, сформованих передавачами на частоті передавального інформаційного сигналу; Вплив комплексу факторів на інформативні параметри корисного сигналу; Відмови у передаванні даних.	Уразливості протоколів; Зловживання ресурсами; Атаки на доступ до мережі; Атаки на криптографію.	Модуляція сигналу із частоним і часовим ущільненням FDD (OFDM, SC-FDMA (частотне розділення одного підканалу з множинним доступом)), TDD; Шифрування; Аутентифікація; Контроль доступу (MAC-фільтрація або алгоритми планування ресурсів); Кодування та корекція помилок; Розподіл частот в мережі LTE в геопросторі.
LTE	Мережевий	Побічні електромагнітні випромінювання; Функціонування поблизу приладів високої напруги як фактору впливу на інформаційний сигнал ; Проблеми з маршрутизацією через неправильну конфігурацію; Втрата пакетів даних.	DoS-атаки; Атаки на протоколи маршрутизації; Атаки на середовище передавання даних; Атаки на профілі безпеки каналу зв'язку.	Використання VPN для шифрування та аутентифікації трафіку; Встановлення фаєрволів для контролю трафіку, що проходить через мережу; Мережеві протоколи безпеки (SSH, SFTP); Алгоритми шифрування; Скремблювання та зашумлення.
GPS	Фізичний	Електромагнітні перешкоди; Атмосферні умови; Неправильна синхронізація годинника в приймачі GPS; Інтерференція від інших пристроїв.	Інтегровані атаки (встановлення шкідливого ПЗ на пристроях GPS або зміна їх фізичних параметрів); Перехоплення сигналу; Фальсифікація сигналу.	Фільтри інтерференції; Шифрування сигналів GPS за допомогою алгоритму AES; Аутентифікація користувачів (використання паролів, сертифікатів); Апаратно-програмний захист від фальсифікації сигналів; Моніторинг і виявлення вторгнень.
GPS	Канальний	Шум і спотворення сигналів; Перешкоди в передаванні сигналів; Міжканальні перешкоди; Вплив погодних факторів; Розрахункові помилки в геопросторі.	НСД до каналу передавання даних GPS; Атаки на перехоплення пакетів.	Корекційні алгоритми; Механізми для компенсації шуму та спотворень сигналів; Використання резервних каналів ; Застосування методів дублювання для забезпечення неперервності зв'язку; Детекція та корекція помилок; Аутентифікація сигналів; Фільтрація і підсилення сигналів.

GPS	Мережевий	Переривання мережевого зв'язку; Зміна умов передавання даних (зміна швидкості передавання даних, втрати пакетів або затримки); Перешкоди у мережевому середовищі; Проблеми маршрутизації; Проблеми зі збереженням даних.	Атаки на протоколи маршрутизації; DoS-атаки ; Атаки на мережеву інфраструктуру.	Резервне копіювання; Відновлення даних; Механізми контролю мережевого зв'язку; Маршрутизаційні протоколи; Механізми виявлення та виправлення помилок в передаванні даних; Використання валідаторів маршрутів для перевірки автентичності та цілісності маршрутів між GPS-приймачами; Контроль доступу.

Таблиця 3

КСБ ACOI кібернетичного простору ІТС на основі моделі STRIDE: апаратні і програмні загрози

КП: ACOI	Модель **S**TRIDE	Загрози		Захист	
		Апаратні	Програмні	Апаратні	Програмні
ACOI	STR**I**DE (конфіденційність)	Фізичний доступ до обладнання; використання несанкціонованих засобів зберігання даних; використання несанкціонованих пристроїв.	Розкриття шифрів криптозахисту інформації; перехоплення інформації під час пересилання/отримання; отримання доступу до конфіденційної інформації.	Контроль процесу передавання; захист обробки даних; створення резервних копій.	Шифрування; передавання інформації; захист доступу до даних; розмежування доступу до об'єктів.
	STRI**D**E (доступність)	Відмова обладнання; перебої в електропостачанні; фізичне пошкодження обладнання.	DDoS-атаки; збої систем архівації даних; відмова програмного забезпечення.	Установка джерел безперебійного живлення; резервне копіювання даних; використання AntiDDos.	Використання механізмів балансування навантаження ; слідкування за підвищенням обсягу трафіку; налаштування обмежень на швидкість запитів до бази даних.
	STRID**E** (авторизація)	Введення невірних даних; внесення несанкціонованих змін в сховища даних; використання фальшивих апаратних компонентів.	Зараження системи комп'ютерними вірусами; модифікація інформації ; слабкі права доступу.	Тестування на проникнення вірусів; резервне копіювання даних; контроль доступу.	Застосування алгоритмів хешування паролів; аутентифікація; реєстрація всіх звернень до інформації, що захищається.

Таблиця 4

КСБ ІП кібернетичного простору кіберфізичної ІТС на рівні фази: апаратні і програмні загрози

КП: ІП – фази	Загрози		Захист	
	Апаратні	Програмні	Апаратні	Програмні
Сприйняття / збір / відбір	Порушення режиму використання інформації; апаратні закладки; недостатня захищеність каналів даних.	Отримання доступу до конфіденційної інформації; розкриття шифрів криптозахисту інформації; атаки спрямовані на розкриття конфіденційної інформації.	Sentinel LDK; Yubikey 5; SecureToken 338M.	ЕЦП; Denuvo; Digify.
Передавання	Затримання передавання повідомлення; збої чи нестабільність роботи технічних пристроїв; приховане перехоплення даних з клавіатури та інших засобів введення інформації.	Отримання несанкціонованого віддаленого доступу; збої програмного забезпечення; відмова програмного забезпечення.	CryptoPhone 600G; Thales nShield; Utimaco.	SASE; CASB; Silent Phone; Signal; Dcrypt XG.

Обробка	Пошкодження обладнання; відмова обладнання; порушення роботи електропостачання.	Порушення цілісності інформації; втрата (знищення) інформації; вірусні атаки.	Gemalto SafeNet; Yubico YubiHSM; Futurex Excrypt.	Cryptomator; BestCrypt; Symantec End-point Encryption.
Зберігання	Фізичне руйнування системи; стихійні лиха; порушення роботи електропостачання.	Знищення інформації зловмисником; порушення цілісності інформації; порушення конфіден-ційності інформації.	SecureToken 338s; Apacer AH651; HIKVISION HS-USB-M200F.	VeraCrypt; DiskCryptor; FileVault.
Представлення / вплив	Втрата потужності; фізичні крадіжки даних; фізичне пошкодження або знищення даних.	Несанкціоновані зміни у файлах; модифікація (спотво-рення) інформації; зараження системи ком-п'ютерними вірусами.	SecureToken 338M; Yubikey 5; Apacer AH651.	Widevine; CapLinked; Sentinel One.

Таблиця 5

КСБ ІП кібернетичного простору кіберфізичної ІТС на етапі операцій : апаратні і програмні загрози

КП: ІП – операції	Загрози		Захист	
	Апаратні	Програмні	Апаратні	Програмні
Збір / відбір даних	Завади в лініях зв'язку від впливів зовнішніх факторів; зчитування інформації з ка-налу передавання за допо-могою електромагнітних наведень; стихійні лиха.	Порушення конфіденційності інформації; порушення достовірності інформації.	Sentinel LDK; Yubikey 5; SecureToken 338M.	ЕЦП; Denuvo; Digify.
Сортування даних	Втрата інформації; витік інформації; відмова систем живлення.	Порушення цілісності інформації; збої програмного за-безпечення при вели-ких навантаженнях.	OnlyKey FIDO2; MIKROTIK WOOBM-USB; ProtectServer HMS.	КриптоПро CSP 5.0; AxCrypt; Cryptomator.
Захист даних	Виведення з ладу системи захисту інформації; апаратні закладки; недостатня захищеність ка-налів даних.	Розкриття шифрів криптозахисту інфор-мації; обхід стандартних за-собів управління без-пекою; приховане перехоп-лення даних з клавіа-тури та інших засобів введення інформації.	ProtectServer HSM; KOKON-R; M-575.	CrowdStrike; Secret Disk Server NG; FileVault.
Транспортування даних	Затримання повідомлення; збої чи нестабільність ро-боти технічних пристроїв; вимкнення фізичних кана-лів передавання даних.	Отримання несанкціонованого віддаленого доступу; перехоплення інформації під час транспортування.	Гряда-301; Бар'єр-301; Канал-301.	TLS; PPTP; SSL; IPsec.

Таблиця 6

КСБ ІП кібернетичного простору кіберфізичної ІТС етапі обробки: апаратні і програмні загрози

КП: ІП - обробка	Загрози		Захист	
	Апаратні	Програмні	Апаратні	Програмні
Автоматизована обробка	Пошкодження та відмова обладнання; порушення роботи електропо-стачання.	Несанкціоноване встановлення зв'язку; збої програмного забезпечення.	Gemalto SafeNet; Yubico YubiHSM; Futurex Excrypt.	Cryptomator; BestCrypt; Symantec Endpoint Encryption.
В режимі реального часу	Завади в лініях зв'язку від впли-вів зовнішніх факторів; зчитування інформації з ка-налу передавання за допомогою електромагнітних наведень;	Втручання в пере-давання даних; копіювання/підро-бка ідентифікаторів віддаленого доступу.	Luna SA; Luna XML; Luna CA4.	ESET End-point Encryption; ESET; JM-Crypt; Silent Phone.

Послідовна	Втрата потужності; фізичні крадіжки даних і устаткування; фізичне пошкодження.	Порушення цілісності інформації; порушення конфіденційності інформації; втрата (знищення) інформації.	OnlyKey FIDO2; Utimaco; Protect Server HMS;	Encrypt Easy; Thales; Secret Disk Server NG.
Хмарні обчислення	Затримання повідомлення; збої чи нестабільність роботи технічних пристроїв; вимкнення фізичних каналів передавання даних.	Отримання несанкціонованого віддаленого доступу; перехоплення інформації під час транспортування.	Гряда-301; Бар'єр-301; Канал-301.	TLS; PPTP; SSL; IPsec;

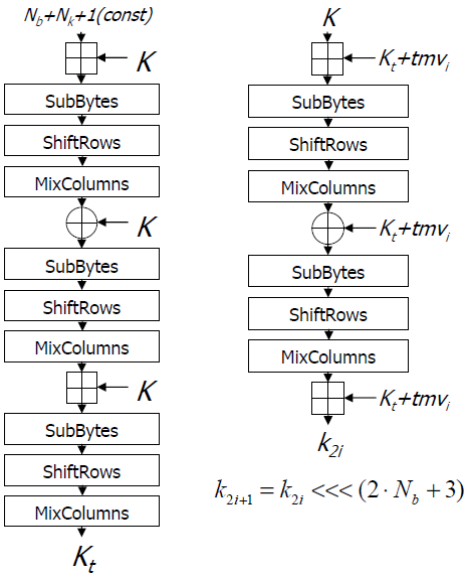


Рис. 6. Блок-схема генерації раундових ключів

Інтерфейс програмної реалізації шифрування даних на основі алгоритму "Калина" в безпровідній мережі LTE кіберфізичної ІТС показано відповідно (рис. 7, 8).

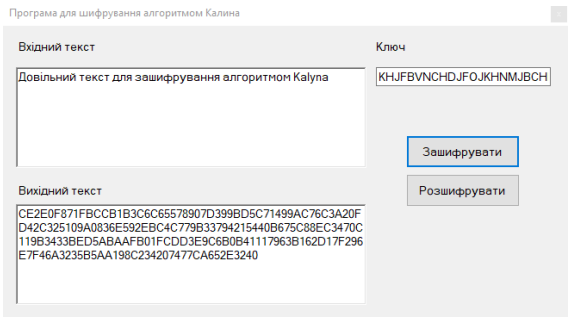


Рис. 7. Результат виконання програми шифрування даних

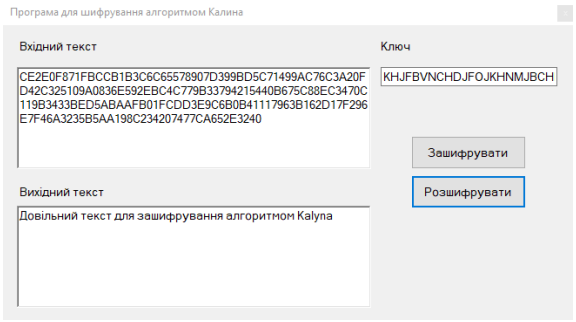


Рис. 8. Результат виконання програми дешифрування даних

Висновки. Розглянуто актуальність Концепції Індустрії 4.0. в Україні в просторі інтелектуалізації транспортної інфраструктури. Проаналізовано розвиток підходів до використання безпечних технологій пітримки функціонування інтелектуальної транспортної системи, зокрема на основі кіберфізичних систем. Запропоновано комплексну багаторівневу модель безпеки кіберфізичної інтелектуальної транспортної системи на основі моделі загроз STRIDE та мережевої моделі OSI. Створено комплексні системи безпеки технологій багаторівневої КФС, що убезпечують ІТС. Розроблено програмну реалізацію шифрування повідомлень в безпровідній мережі кіберфізичної ІТС на основі симетричного блокового алгоритму "Калина" засобами мови програмування C#.

Список літератури

[1]. Yurchak Oleksandr. "Ukrayins'ka stratehiya Industriyi 4.0 – 7 napryamiv rozvytku" [Електронний ресурс]. Режим доступу: https://industry4-0-ukraine.com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku.

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

[3]. Valeriy Dudykevych, Ivan Prokopyshyn, Vasyl Chekurin, Ivan Opirskyy, Yuriy Lakh, Taras Kret, Yevheniia Ivanchenko, Ihor Ivanchenko. A multicriterial analysis of the efficiency of conservative information security systems//Eastern-european journal of enterprise technologies. Information and controlling system. Vol 3, No 9(99), pp.6-13, (2019).

[4]. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, I. Opirskyy, O. Milov and others. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p.

[5]. Бобало Ю. Я. Стратегічна безпека системи "об'єкт – інформаційна технологія": [монографія] / [Бобало Ю. Я., Дудикевич В. Б., Микитин Г. В.]. Львів: Видавництво НУ "Львівська політехніка", 2020. 260 с.

[6]. Дудикевич В.Б. Квінтесенція безпеки кіберфізичних систем / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету "Львівська політехніка", Інформаційні системи і мережі. 2018. № 887. С. 58-69.

[7]. Дудикевич В.Б. Системна модель інформаційної безпеки "розумного міста" / В.Б. Дудикевич, Г.В. Микитин, М.О. Галунець // Системи обробки інформації. 2020. Випуск 2(161). С. 93-98.

[8]. Ismaeel Al Ridhawi, Safa Otoum, Moayad Aloqaily, Yaser Jararweh, Thar Baker. Providing secure

and reliable communication for next generation networks in smart cities. Sustainable Cities and Society, 2020, vol. 56.

[9]. Zhili Zhou; Akshat Gaurav; Brij Bhooshan Gupta; Miltiadis D. Lytras; Imran Razzak. A Fine-Grained Access Control and Security Approach for Intelligent Vehicular Transport in 6G Communication System. IEEE Transactions on Intelligent Transportation Systems, 2022, pp. 9726-9735.

[10]. Sita Rani, Aman Kataria, Meetali Chauhan, Punam Rattan, Raman Kumar, Arun Kumar Sivaraman. Security and Privacy Challenges in the Deployment of Cyber-Physical Systems in Smart City Applications: State-of-Art Work. MaterialsToday: Proceedings, 2022, pp. 4671-4676.

[11]. Amit Pundir; Sanjeev Singh; Manish Kumar; Anil Bafila; Geetika J. Saxena. Cyber-Physical Systems Enabled Transport Networks in Smart Cities:

[12]. Challenges and Enabling Technologies of the New Mobility Era. IEEE Access, 2022, pp. 16350-16364.

[13]. Konstantinos Ntafloukas,Daniel P. McCrum and Liliana Pasquale. A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure. Applied Sciences, 2022, p. 9241.

[14]. Oleg Illiashenko, Vyacheslav Kharchenko,Ievgen Babeshko, Herman Fesenko and Felicita Di Giandomenico. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy, 2023, p. 1123.

УДК: 004.054

Dudykevych V., Mykytyn G., Sydoryk D. Building a Comprehensive Multi-Level Security Model for the Cyber-Physical Intelligent Transport System

***Abstract**. The generalized architecture of the Intelligent Transport System (ITS) based on a multi-level cyber-physical system (CPS) has been considered: physical space sensors, wireless communication technologies, automated information processing system (AIPS) of the cyber space. A comprehensive security model for ITS in the "multi-level CPS - multi-level security" space is proposed. Comprehensive security systems (CSS) have been built: for the physical and cyber spaces of the cyber-physical ITS based on the STRIDE threat model at the external level; for the communication environment based on the OSI network model at the internal level. A software implementation of symmetric block message encryption based on the "Kalina" algorithm has been developed using the C# programming language in the communication environment of the ITS.*

***Keywords**: intelligent transport, cyber-physical system, physical space, communication environment, cyber space, multi-level comprehensive security model, comprehensive security system, threats, security technologies, message encryption algorithm.*

Дудикевич Валерій Богданович, доктор технічних наук, професор, керівник Західного регіонального.навчально-наукового центру захисту інформації, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.

Valerii Dudykevych, Doctor of Technical Sciences, Professor, Head of the Western Regional Information Security Training and Research Center, Professor of the Department, Lviv Polytechnic National University, Lviv, Ukraine.

Микитин Галина Василівна, доктор технічних наук, професор, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.

Galyna Mykytyn, Doctor of Technical Sciences, Professor, Professor of Department of Lviv Polytechnic National University, Lviv, Ukraine.

Сидорик Дмитро Олегович, магістрант кафедри захисту інформації Національний університет «Львівська політехніка», Львів, Україна.

Dmytro Sydoryk, Master's student of the Department of Information Security, Lviv Polytechnic National University, Lviv, Ukraine.

Отримано *26 лютого 2023 року,* затверджено редколегією *1 квітня 2024 року*