**УДК 004.5, 004.7**

**М.В. Торський, Я. С. Парамуд**

Національний університет “Львівська політехніка”,

кафедра електронних обчислювальних машин

**ПРИНЦИПИ МОНІТОРИНГУ ТА КЕРУВАННЯ МЕРЕЖЕЮ ЗАРЯДНИХ СТАНЦІЙ ЕЛЕКТРИЧНИХ АВТОМОБІЛІВ**

© *Торський М.В., Парамуд Я. С., 2020*

**Розглянуто принципи побудови, моніторингу, організацію та систему безпеки у мережі зарядних станцій електричних автомобілів. Приводиться опис процесу взаємодії системи з серверною системою.**

**Ключові слова: мережа зарядних станцій, зарядна станція, сервер, моніторинг, кібербезпека.**

**Torskyi M., Paramud Y.**

Lviv Polytechnic National University,

Computer Engineering Department

**PRINCIPLES OF MONITORING AND CONTROL OF THE NETWORK OF CHARGING STATIONS OF ELECTRIC VEHICLES**

© *Torskyi M., Paramud Y., 2020*

**This paper describes the principles of construction, monitoring, organization, and safety systems in the networks of electric car charging stations are considered. Provides a description of the process of interaction of systems with the server system.**

**Keywords: charging station network, charging station, server, monitoring, cybersecurity.**

**Вступ**

Електромережі з підключеними до них електричних автомобілів (ПЕА) поширюється по всьому світу. З цим, оптимальне управління зарядом ПЕА стає важливим фактором для власників ПЕА, постачальників послуг, комунальних підприємств та роботи енергосистеми. Для належного управління навантаженнями ПЕА необхідна інтелектуальна система управління зарядом, яка здатна оптимізувати зарядку ПЕА на загальнодоступних зарядних станціях та будується на принципах кіберфізичних систем.

Кіберфізичні системи - системи з тісною інтеграцією обчислювальних, комунікаційних та керуючих систем (кіберпростір) та фізичних процесів, які можуть взаємодіяти з людьми за допомогою багатьох способів. Фізичні процеси впливають на обчислення і навпаки. Здатність взаємодіяти і розширювати можливості фізичного світу шляхом обчислення та контролю є ключовим фактором для технологічних розробок. Розвиток кіберфізичних систем викликає специфічні проблеми, які рідко зустрічаються в інших дисциплінах інженерії програмного забезпечення, таких як корпоративні програми та веб-розробки. Ці проблеми здебільшого походять від стійкої взаємодії таких систем з реальним світом через недосконалі сенсори та акторів під час впливу середовища та фізичних законів [1,2]. Для вирішення цих проблем існує підхід exidaR, який складається з чотирьох рівнів:

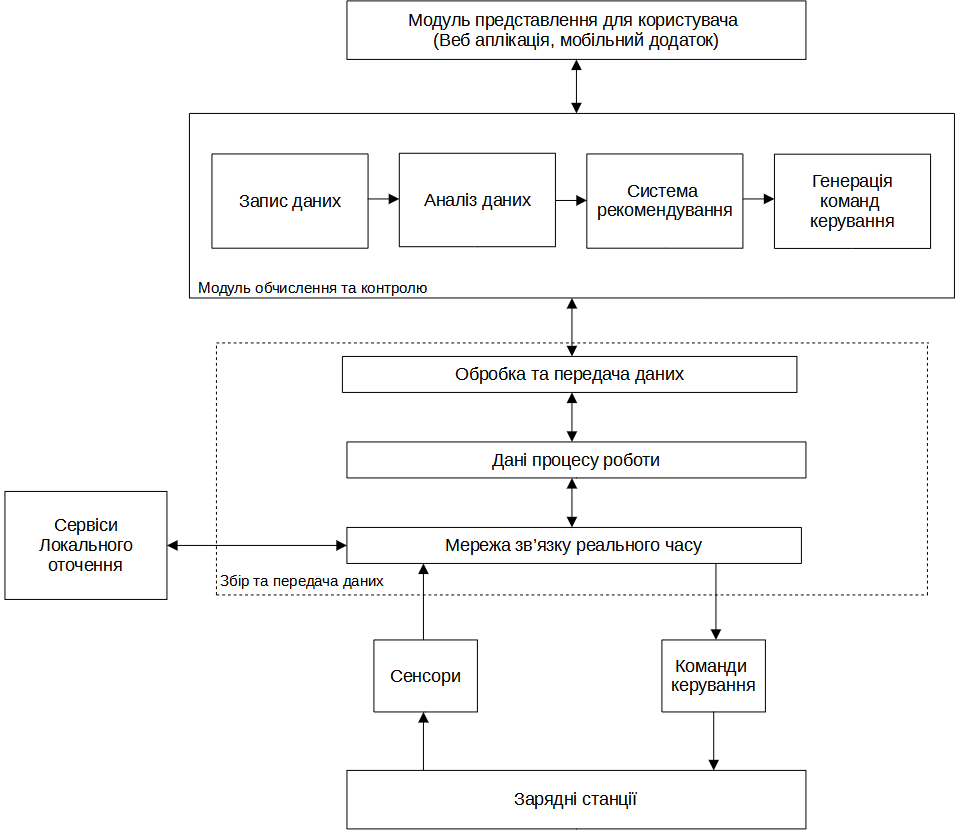
● Об'єкт відображення (текстові вимоги та випадки використання),

● Логічний рівень, конкретні технічні концепції (абстрактні C&C моделі, діаграми діяльності детерміновані C&C моделі),

● Реалізація (наприклад, ECU, CAN-BUS, Flexray і синхронізація). Сильні сторони моделювання C&C на логічному рівні містять здатність описувати архітектури компонентами, що виконують обчислення та інформаційні потоки, модельовані через з'єднувачі між їх інтерфейсами. Парадигма фокусується на особливостях програмного забезпечення та їх логічній взаємодії. Завдяки ієрархічній декомпозиції компонентів, великі та складні системи можуть бути розроблені зацікавленими сторонами способом поділу [3]. Інтеграція хмарних і бездротових мереж датчиків також є важливою частиною кібер-фізичних систем[7]. КФС забезпечує характеристики мережевої інтеграції, такі як методи контролю доступу до ЗМІ та їх вплив на системну динаміку, проміжне програмне забезпечення та програмне забезпечення, що забезпечує координацію мережевого контролю над тимчасовою синхронізацією мережевих транзакцій і допуском відмов [4]. Взаємодія людини і системи: Моделювання та вимірювання ситуативної обізнаності людиною системи та її екологічних змін у параметрах є критичними для прийняття рішень. Робота з невизначеністю: визначеність - це процес надання доказів того, що дизайн є дійсним [5].

1. **Об’єкт дослідження та його технологічний аудит**

На рис. 1 представлено схему кіберфізичної системи. Об’єктом дослідження є зарядна станція для електричних автомобілів та інших електричних транспортних засобів, яка є одним з функціональних блоків, що працюють у складі кіберфізичної системи.



**Рис. 1** Базова структура кіберфізичної системи керування мережею зарядних станцій

На основі аналізу можна сформулювати загальний процес роботи мережі зарядних станцій для електричних автомобілів:

1. Система проводить постійний аудит компонентів системи (інформація про справність та завантаження зарядних станцій, наявність електромережі/напруги від сонячних панелей та наявність заряду у накопичувачі) для актуальності даних у користувацьких додатках.
2. Водій користуючись веб додатком або мобільною аплікацією бронює зарядну станцію відповідно до конфігурації зарядного пристрою автомобіля. Прибувши до місцезнаходження станції авторизується пристроєм за допомогою створеного ключа.
3. Користувач отримує дозвіл на підключення, після підключення система сповістить шляхом надсилання push-повідомлення на смартфон користувача про час, що знадобиться для заряджання автомобіля.
4. Зарядний пристрій впродовж кожного етапу комунікації з користувачем надсилає дані про стан роботи на сервер, таким чином в разі помилки реагування системи стає більш оперативним. Дані про весь цикл використання системи записуються у базу даних для подальшого їх аналізу.
5. Після проведення аналізу даних система може генерувати рекомендаційні рішення для оптимізації роботи системи.

На сьогоднішній день існують багато типів зарядних станцій з різними характеристиками від різних виробників, про мережі зарядних пристрої для електричних автомобілів, приватні зарядні станції та перспективи розвитку наведено у роботі [11]. Проблема виникає при об’єднанні цих зарядних станцій в спільну мережу, моніторингом системи, що може призвести до фінансових втрат, а також з доступністю даних та можливостей для користувачів.

**2. Мета та задачі досліджень**

Метою роботи є аналіз принципів моніторингу в тому числі розробка структурної схеми та моделі кіберфізичної системи, яка буде забезпечувати необхідну продуктивність заряджання споживачам та яку необхідно інтегрувати в 5-ти рівневу платформу кіберфізичної системи.

Для досягнення поставленої мети необхідно виконати наступні задачі:

1. Визначити який тип, перелік та необхідні параметри, для роботи у складі зарядної станції.
2. Змоделювати можливі запити клієнтів до системи.
3. Розробити імітаційну модель зарядної станції, яка дозволить вибрати конфігурацію, що задовольняє запити клієнтів.
4. На основі імітаційної моделі розробити модуль аналізу даних, який дозволяє генерувати рекомендовані рішення щодо розташування зарядних станцій та оновлення їх обладнання, а також можливої зміни їх конфігурації.

**3. Дослідження існуючих рішень проблеми**

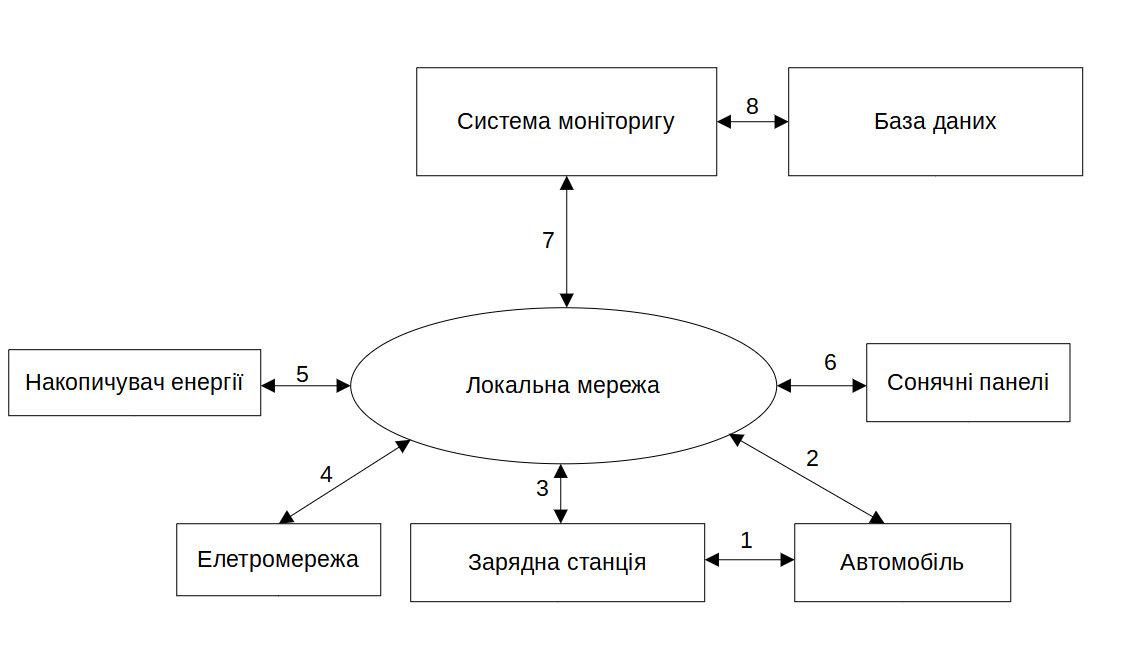
В останні роки електромобілям приділяється значна увага як екологічно стійкого і економічно ефективного замінника транспортних засобів з двигуном внутрішнього згоряння, для вирішення проблеми залежності від видобувного палива та для скорочення викидів парникових газів. [1] Зарядні станції для цих автомобілів містять комп'ютери, підключені до Інтернету. Ці системи виконують важливі функції управління, як авторизація, зарядка електромобілів та підключення до місцевої електромережі. Зарядні станції дозволяють користувачам та транспортним засобам використовувати Bluetooth або Wi-Fi. [2]

У роботі [1] розглядають основні види зарядних станцій за європейськими стандартами (CENELEC and ETSI (M/468)), а також включає короткий зміст можливих типів систем накопичення енергії (СНЕ) та можливого планування зарядних станцій, включаючи їх. В [3] розглядають розробку самоадаптивних КФС з використанням цільового моделювання та звертають увагу на те, що такий підхід часто призводить до неправильної конфігурації при виконанні. У роботі [10] описано особливості застосування стандартизованих інтерфейсів обміну інформацією у кіберфізичних системах . У роботі [4] досліджено існуючу роботу з кібербезпекою у розумній системі управління зарядкою, основні кіберфізичні атаки з різними наслідками та основні проблеми боротьби з цими атаками. Підсумовуючи, зазначимо основні вимоги до проектування: швидке заряджання електромобіля; робота в складі КФС; визначити певну кількість типових конфігурацій, які будуть оптимально адаптовані до інтенсивності використання, зібрання статистики та забезпечити захист від можливих кібератак.

**4. Методи досліджень**

**4.1. Загальна структура мережі зарядних станцій**

На основі досліджень функціональних задач КФС зарядних станцій розроблено структуру функціональних зв'язків мережі зарядних станцій яка приведена на рис. 2. Система включає вимоги забезпечити безпеку зарядного пристрою, всіх функцій, що необхідні для налаштування безпечних операційних процесів [16].



**Рис. 2** Структура функціональних зв'язків мережі зарядних станцій

Розглянемо основні елементні зв’язки:

1 - Отримання автомобілем послуг зарядної станції;

2 - Вибір та навігація клієнта до зарядної станції за допомогою додатку;

3 - Отримання та передача даних зарядної станції до системи моніторингу;

4 - Отримання інформації про наявність та постачання електроенергії від електромережі;

5 - Отримання інформації про наявність та постачання електроенергії від накопичувача у разі відмови систем енергопостачання;

6 - Отримання інформації про наявність та постачання електроенергії від сонячних панелей;

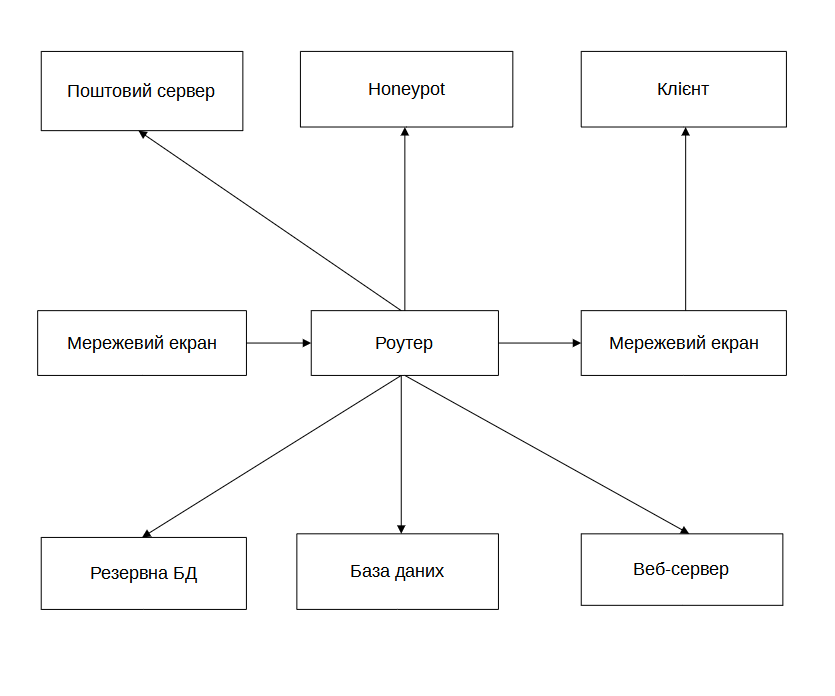
7 - Система моніторингу обробляє інформацію від усіх частин мережі, а також відсилає команди управління вузлами системи;

8 - Система моніторингу зберігає інформацію про наявні зарядні станції, їх статус та результати роботи;

У роботі досліджується програмна складова: організація комп’ютерної системи керування зарядною станцією для електричних автомобілів, а також серверна обробка даних, їх взаємодія із зарядною станцією, можливі методи захисту від кібератак.

**4.2 Сервер та клієнтська частини**

Програмне забезпечення на зарядній станції включає програмне забезпечення, що працює на платі, яка посилає контрольні сигнали на зарядну станцію, інтерфейс управління зарядною станцією, мобільні програми та інтерфейс програмування програм забезпечується зарядними станціями. Більшість зарядних станцій також забезпечити сервер зарядної станції, який зв'язується зі станцією через Інтернет. Інформацію про стандартизовані інтерфейси обміну інформацією у кіберфізичних системах наведено у роботі [9]. На рис 3 наведено структурну схему зв’язків серверної частини.

****

**Рис. 3** Структурний рівень веб системи

Серверна система складається з кількох серверів та вузла збереження інформації, бази даних. Роутер виконує функцію зв’язку з зарядним станціями, що дозволяє опрацьовувати платежі, передачу конфігураційних налаштувань, організацію збереження статистичних даних впродовж повного циклу роботи зарядної станції. Зв’язок встановлюється не напряму, а за допомогою додавання проміжного вузла у вигляді мережевого екрану (фаєрволу). Поштовий сервер використовується для відправлення push-повідомлень клієнту про стан процесу зарядки, а також для повідомлення техпрацівникам про стан зарядної станції.

Сервер бази даних і резервний сервер бази даних забезпечують необхідну функціональну потужність та надійність збереження інформації під час роботи системи, резервна база даних копіює дані основної не включаючись напряму у роботу системи, допоки основний сервер бази даних не вийде з ладу.

Веб-сервер відповідає за представлення клієнту всіх функціональних можливостей системи, а також метод зв’язку з техпідтримкою у разі необхідності. За умови, що електромобілі заряджаються у режимі розумної зарядки, контрольовано, немає підстав сумніватись, що функціонування ринкових сил перетворить електромобілі на конкурентоспроможну транспортну технологію. З часом ринок покаже, які функції та засоби зарядки бажають та готові платити клієнти електромобілів, система пропонує власникам усіх видів зарядних станцій надавати доступ до них за допомогою системи.

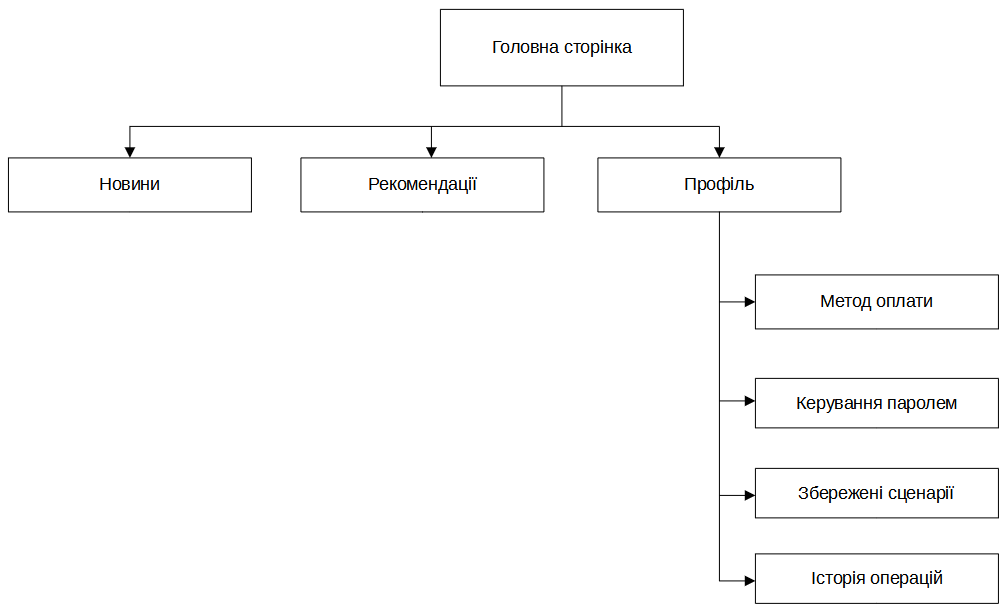
Honeypot сервер використовується для привернення уваги зловмисника та стає ціллю атаки на систему, не становлячи при цьому жодної небезпеки для мережі. Для зменшення ризику можливих атак у всіх відкритих каналах зв’язку мережі використовується шифрування. Основними завданнями серверної частини є:

1. Контроль оплати
2. Моніторинг стану

Контроль оплати системи забезпечує передачу на сервер форму трансакції підтвердження оплати або отримання послуг. Моніторинг стану виконує функцію контролю зарядних станцій у режимі реального часу. Стани зарядних станцій:

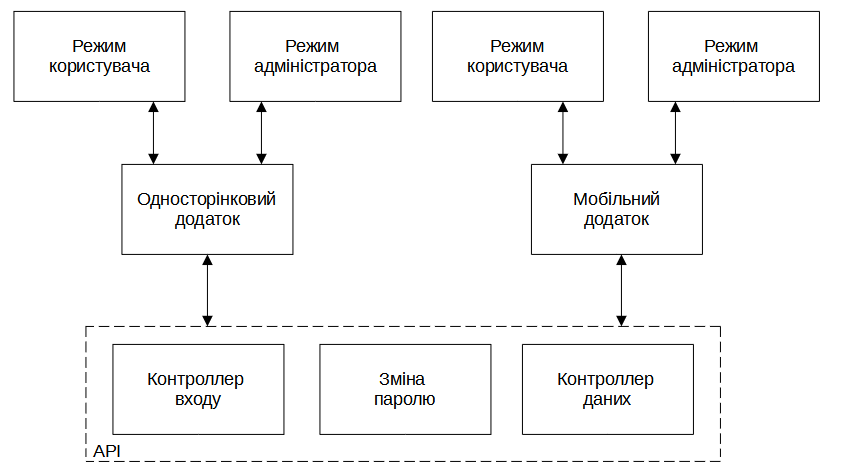
1. доступні
2. недоступні
3. несправні
4. призупинені
5. зарядка
6. підготовка
7. обробка

На рис 4 наведено структуру клієнтської аплікації:

**Рис. 4** Структура клієнтського веб додатку системи керування

Веб додаток складається з декількох сторінок, оперування даними відбувається через API серверної частини. Головна сторінка використовується для візуалізації доступних зарядних станцій поряд з користувачем, використовуючи функцію геолокації. Сторінка рекомендацій дозволяє переглянути найближчі доступні станції, що є сумісними з автомобілем користувача, у разі виникнення складностей надається можливість пошуку вручну. Сторінка історії операцій надає можливість перегляду всіх закінчених циклів взаємодії з системою. Сторінка збережених сценаріїв дозволяє звернутись до станцій за раніше закінченим сценарієм. Керування паролем дозволяє змінити пароль або збільшити рівень захисту додавши опцію подвійної верифікації. Сторінка новин дозволяє переглянути оголошення та список нещодавно доданих у систему станцій.

На рис 5 наведено структурну схему зв’язків клієнтської частин:



**Рис. 5** Структура зв'язків клієнтської частини

Користуючись веб додатком або мобільною аплікацією режим користувача надає змогу переглядати контент додатку (переглянути доступні пристрої, бронювати зарядну станцію). Режим адміністратора надає змогу редагувати наповнення додатку: видалити неробочий пристрій, оновити оголошення в розділі новин, заблокувати користувача.

**Взаємодія зарядних станцій з сервером**

Зв’язок між системою керування та зарядними станціями відбувається за допомогою протоколу OCPP, що дозволяє цим складовим взаємодіяти між собою, утворюючи відкриту платформу. Протокол надає наступні можливості:

1. Авторизація користувача для початку стягнення плати, включаючи локальний список авторизації;
2. Віддалена зміна конфігурації зарядного пристрою, стан зарядних станцій;
3. Передача даних сеансу зарядки в режимі реального часу до центральної системи управління;
4. Віддалене управління сеансом зарядки (початок / кінець);
5. Розумна зарядка;
6. Дає змогу підключення будь-якої центральної системи управління до будь-якої зарядної станції;

Можливість оптимально планувати зарядку електромобілів, щоб максимізувати використання санкціонованої електричної енергії від мережі. Розумна зарядка максимізує кількість електромобілів, з яких можна стягувати плату одночасно, обмежуючи контрактний попит. Це допомагає підвищити стабільність мережі.

**Безпека у мережі зарядних станцій електричних автомобілів**

В системах зарядних станцій є багато сенсорних, комунікаційних та обчислювальних компонентів, які потенційно вразливі до атак кібербезпеки. Ці вразливості потенційно можуть бути використані хакерами, щоб порушити доступність, цілісність та конфіденційність мережі зарядних станцій або навіть електромережі. З огляду на надзвичайне зростання ринку електромобілів у найближчі кілька років, важливо розробити надійні зарядні станції. Проектування надійних зарядних станцій вимагає більш глибокого розуміння кіберфізичної взаємодії зарядної станції, а також того, як кібер- та фізичні компоненти впливають один на одного.

Зарядні станції стикаються із загрозами безпеки своїх компонент внутрішнього зв'язку, включаючи радіостанції, придорожню інфраструктуру та інші транспортні засоби.

У деяких автомобілях оновлення відбувається вручну за допомогою USB-накопичувача. Однак бездротовому методу надають перевагу над ручним виправленням через його економічну ефективність та швидку доставку. З іншого боку, ця бездротова передача даних відкриває широку поверхню атаки [8, 10].

Існує дві різні категорії точок входу, які можуть бути використані для компрометації безпеки системи зарядних станцій, а саме, точки входу на основі мережі фізичні точки доступу, наприклад через зарядний порт або шляхом втручання в апаратне забезпечення пристроїв. У цій роботі увага зосереджена саме на мережевих атаках. Сучасні зарядні пристрої оснащені бездротовим або дротовим модулем зв’язку, наприклад Wi-Fi та LAN відповідно. Модуль зв'язку дозволяє авторизованим користувачам ініціювати сеанс зарядки та повідомте про стан заряду сеансу до оператора станції. Така передача даних може відбуватись через модулі в транспортному засобі або смартфоні, вразливість комунікацій різних типів добре описана у [5-7]. Порушення безпеки будь-якої з цих мереж через погану автентифікацію або відсутність шифрування може вплинути на всі підключені зарядні станції у мережі. Тему атак перерозподілу навантаження в енергосистемах добре розкрито у роботі [14]. Також у роботі [15] описано метод NFC Peer-to-Peer атак. Методи мережевих атак системи:

1. Зловмисне програмне забезпечення: погана реалізація різних програм безпеки програмні модулі в зарядній станції та хмарі може бути використаний для запуску більш складних атак що встановлюють шкідливе програмне забезпечення;
2. Man-in-the-Middle: при такому типі атаки зловмисник намагається перехопити трафік та заблокувати приймач, маючи при цьому доступ до переданого трафіку, дозволяє зловмиснику діяти як ретранслятор між відправником і одержувачем без відома жодної сторони, зловмисник може пошкодити дані або взяти повний контроль над вузлом і змінити статус одного з цих вузлів для передачі неправильної інформації про стан зарядного пристрою;
3. Відмова в обслуговуванні: скомпрометовані облікові дані користувача та станції можуть бути використані для запуску дуже складних атак DOS.

Враховуючи складну та щільну інтеграцію апаратних засобів та програмного забезпечення, деякі програмні атаки також можуть бути здійснені через апаратне забезпечення. Доступно багато контрзаходів автентифікації та перевірки програмного забезпечення на різних етапах роботи станції, таких як запобігання втручанню в програмне забезпечення та забезпечення бутстрепінгу [8]. Напади різних типів спрямовані на зарядну станцію або оточуючу інфраструктуру, включаючи електромережу, можуть мати погані наслідки з точки зору впливу на безпечний та надійний процес зарядки.

**Висновки**

У цій роботі розглянуто структуру мережі зарядних станцій електричних автомобілів, структуру серверної частини та нововведення у контролі та пропозицій для користувачів, запропоновано структуру системи з використанням сучасних технологій конфігурації та зв’язку. Розглянуто різні типи вразливостей та атак, а також підходи до поліпшення безпеки у мережі зарядних станцій електричних автомобілів. Розроблено структуру та внутрішню організацію клієнтської частини системи. Мета системи керування розумними зарядними станціями полягає не тільки в оптимізації зарядки великої кількості електричних автомобілів, але і надання багатьох мережевих послуг. Тому належні алгоритми слід розробляти шляхом подальших досліджень та розробок таких мереж.

*1. Melnyk A. O. Multilevel basic cyber-physical system platform : Cyber-physical systems: achievements and challenges. First scientific seminar materials (June 25-26 2015 Lviv). – 2015. – p. 5–15 2. Falvo, Maria Carmen, et al. "EV charging stations and modes: International standards." Power Electronics, Electrical Drives, Automation, and Motion (SPEEDAM), 2014 International Symposium on. IEEE, 2014. 3. Raju Gottumukkala, Rizwan Merchant, Adam Tauzin, Kaleb Leon, Andrew Roche, Paul Darby, "Cyber-physical System Security of Vehicle Charging Stations" April 2019 4. Amal Ahmed Anda and Daniel Amyot "Arithmetic Semantics of Feature and Goal Models for Adaptive Cyber-Physical Systems" Sep 2019 5. "Cybersecurity of Electric Vehicle Smart Charging Management Systems", Aug 2020 6. Kocher, Paul, et al. "Security as a new dimension in embedded system design." Proceedings of the 41st annual Design Automation Conference. ACM, 2004. 7. Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." USENIX Security Symposium. 2011. 8. Salo A.M. "Simulation of automatic water purification for vending cyberphysical systems." 2018 9. “Features of classification and application of telecommunication interfaces in cyberphysical systems“ Miyushkovich E.G.* Paramud Y*.S. 2015. 10. Samrat Acharya, Yury Dvorkin, Ramesh Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?" 27 Feb 2020 11. Facilitating e-mobility: EURELECTRIC views on charging infrastructure, EURELECTRIC Position Paper, March 2012. 12. O. Veneri, L. Ferraro, C. Capasso, D. Iannuzzi, “Charging Infrastructures for EV: Overview of Technologies and Issues”, 2012 IEEE ESARS, Electrical Systems for Aircraft, Railway and Ship Propulsion Conference, Oct. 2012. 13. M.C. Falvo, L. Martirano, D. Sbordone, and E. Bocci, "Technologies for Smart Grids: a brief review". Proc. IEEE EEEIC 2013, 12th Int. Conf. on Environment and Electrical Engineering. 14. Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 382–390, 2011. 15. Francis, Lishoy, et al. "Practical NFC peer-to-peer relay attack using mobile phones." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg, 2010. .16. European Network for Cyber Security, “EV charging systems security requirements,” 2017.*