Разінкін Нікіта Сергійович
асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ПРОЦЕСІ ФУНКЦІОНУВАННЯ ЕЛЕКТРОМОБІЛЬНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

DOI https://doi.org/10.36059/978-966-397-537-5-11

У сучасних умовах стрімкого розвитку електромобільної інфраструктури в Україні, зумовленого глобальними тенденціями декарбонізації транспорту, сталого розвитку та зростання популярності електротранспорту, питання захисту інформації набуває критичного значення. Електромобільна інфраструктура, що охоплює зарядні станції, системи керування зарядкою, мобільні додатки та енергетичні мережі, є складною кіберфізичною системою, яка потребує надійного захисту від кіберзагроз. В Україні, де кількість електромобілів стрімко зростає, а зарядна мережа розвивається нерівномірно, виникають унікальні виклики, пов'язані з обмеженою інфраструктурою, низьким рівнем цифрової грамотності та нестабільністю енергосистеми. Недостатня стандартизація безпеки, вразливості в протоколах зв'язку, а також слабкий захист мобільних додатків створюють ризики несанкціонованого доступу, фінансових втрат і навіть дестабілізації енергомережі. У цьому контексті впровадження комплексних заходів захисту інформації, гармонізованих із міжнародними стандартами є необхідним для забезпечення стабільності, безпеки та сталого розвитку електромобільної інфраструктури.

Питання організації захисту інформації в процесі функціонування електромобільної інфраструктури в Україні привертало увагу багатьох науковців, серед яких Алімурадов Ш. Р., Хуан І., Аянович А., Хаас Р., Чжан, Півняк Г., Козак Ю., Семенов В., Джонсон Дж. та інші. Проте, незважаючи на значний науковий доробок, проблема забезпечення ефективного кіберзахисту електромобільної інфраструктури залишається не до кінця вирішеною. Це зумовлено стрімкою еволюцією кіберзагроз, які стають дедалі складнішими та різноманітнішими, зокрема через використання вразливостей у протоколах передачі даних, мобільних додатках

і кіберфізичних системах. Наприклад, атаки типу «людина посередині», “juice jacking” чи масові зарядні атаки можуть дестабілізувати енергомережу та спричинити економічні збитки. Така динаміка загроз вимагає комплексного підходу до вдосконалення технічних, організаційних і регуляторних заходів захисту, особливо з урахуванням специфіки української інфраструктури, яка характеризується нерівномірним розподілом зарядних станцій і обмеженою цифровою грамотністю населення. Отже, дослідження питань кіберзахисту електромобільної інфраструктури в Україні зберігають високу актуальність, спрямовану на забезпечення її стійкості та інтеграцію з міжнародними стандартами безпеки.

Мета роботи полягає у розробці структурованого плану впровадження змін до організації захисту інформації в процесі функціонування електромобільної інфраструктури в Україні, спрямованого на підвищення кібербезпеки, гармонізацію з міжнародними стандартами безпеки та адаптацію до локальних умов, враховуючи технічні, організаційні та регуляторні аспекти, для забезпечення стабільності енергетичної системи, захисту даних користувачів і запобігання кіберзагрозам.

Для досягнення поставленої мети було виконано наступні завдання:

– визначити основні кіберзагрози, що впливають на електромобільну інфраструктуру в Україні з урахуванням локальних особливостей енергосистеми;

– проаналізувати міжнародні стандарти безпеки та розробити пропозиції щодо їх гармонізації з національною нормативно-правовою базою для створення єдиних стандартів захисту електромобільної інфраструктури в Україні;

– оцінити організаційні заходи з урахуванням низького рівня цифрової обізнаності в Україні;

– запропонувати технічні рішення для створення систем моніторингу в реальному часі та децентралізованих CMS, які забезпечать виявлення аномальної активності, захист від масових зарядних атак і підвищення стійкості інфраструктури до збоїв;

– дослідити можливості міжнародної співпраці для отримання фінансування, технологій і експертизи.

Об’єктом дослідження виступає електромобільна інфраструктура в Україні, включаючи зарядні станції, системи керування зарядкою, мобільні додатки та протоколи передачі даних.

Предмет дослідження – організація захисту інформації в процесі функціонування електромобільної інфраструктури, спрямована на підвищення кібербезпеки, гармонізацію з міжнародними стандартами та адаптацію до локальних умов.

У контексті сучасних тенденцій сталого розвитку, глобальної декарбонізації транспорту та інтенсивного впровадження електротранспорту, електромобільна інфраструктура виступає як фундаментальна передумова ефективного функціонування електромобілів у міському та міжміському середовищі. Незважаючи на широке використання терміну, у науковій літературі відсутнє єдине універсальне визначення електромобільної інфраструктури, що зумовлено складністю, міждисциплінарністю та динамічністю цієї сфери.

Згідно з дослідженням Алімурадова Ш. Р. [1], електромобільна інфраструктура – це сукупність технічних, організаційних та інформаційних засобів, які забезпечують можливість заряджання, обслуговування та експлуатації електромобілів у певному просторі. Це визначення підкреслює багатокомпонентність системи, де інфраструктура не обмежується лише зарядними станціями, а включає енергетичну інфраструктуру, логістичну підтримку, цифрову платформу управління та навіть регуляторні елементи.

Дослідники Хуан І. та ін. розширюють це поняття, розглядаючи ЕМІ як інтелектуальну та інтегровану систему, що пов'язує електротранспорт, енергетичні мережі та інформаційні технології [2]. Вони пропонують розглядати електромобільну інфраструктуру як кібер-фізичну систему, що дозволяє оптимізувати навантаження на енергомережу, забезпечити гнучке заряджання та реалізувати концепцію Vehicle-to-Grid. У цьому контексті важливо зазначити, що ЕМІ – це не лише фізична інфраструктура, а й логіка взаємодії між користувачами, транспортними засобами та енергосистемою.

З методологічної точки зору, науковці пропонують класифікацію електромобільної інфраструктури за функціональними ознаками. Так, дослідження Аяновича А. та Хааса Р. поділяє інфраструктуру на:

– зарядну (charging infrastructure);
– сервісну (maintenance infrastructure);
– комунікаційну (digital infrastructure);
– регуляторну (policy and regulatory infrastructure) [3].

Це дає змогу комплексно аналізувати стан і розвиток електромобільної інфраструктури у різних країнах, зокрема з урахуванням інституційного та технологічного контексту.

Окремої уваги заслуговує питання просторової доступності ЕМІ, яке, як зазначає Чжан та ін., безпосередньо впливає на швидкість прийняття електромобілів населенням [4]. Автори стверджують, що розміщення зарядних станцій має базуватися на моделюванні мобільності, інтенсивності трафіку та енергетичних обмежень. Це визначає необхідність синергетичного підходу між урбаністикою, енергетикою та транспортним плануванням.

Жаровська І., Козак Ю., Семенов В. наголошують, що в умовах України ЕМІ набуває особливого значення через високий рівень імпорту електромобілів, нерівномірний розподіл зарядної мережі та залежність від нестабільної енергосистеми [5]. Зокрема, вказується на важливість включення до ЕМІ альтернативних джерел енергії (сонячні панелі, акумуляторні буфери), що дозволяє створити енергетично незалежні зарядні хаби.

Функціонування електромобільної інфраструктури в Україні має багатовимірний характер, що включає технічні, економічні й нормативно-правові аспекти. Перш за все, стрімкий ріст кількості електромобілів у країні зумовлює значні зміни у транспортній екосистемі та потребує формування нової інфраструктури обслуговування. З 2010 до 2022 року Україна демонструє стійку тенденцію нарощування ринку електромобілів – з первинних імпортних партій у кількості близько 3,2 тисячі одиниць за 2010–2016 роки до більш ніж 25 850 автомобілів станом на 1 січня 2021 року. Основну долю становлять Nissan Leaf, Tesla Model S, Renault Kangoo та BMW i3, що складає понад 60 % у загальній структурі продажів [6].

Важливим фактором є територіальна нерівномірність розвитку: найбільше електромобілів зареєстровано в Києві й Київській області, Одеській, Харківській, Дніпропетровській і Львівській областях, як зображено на рис. 1.

Така концентрація пояснюється вищим рівнем доходів населення, наявністю зарядної інфраструктури та транспортною політикою регіонів. Функціонування інфраструктури не відбувається автоматично, а супроводжується комплексною взаємодією між виробниками

транспортних засобів, їхніми дилерами, сервісними центрами, операторами зарядок, енергокомпаніями, органами влади, банківськими і фінансовими установами [7].

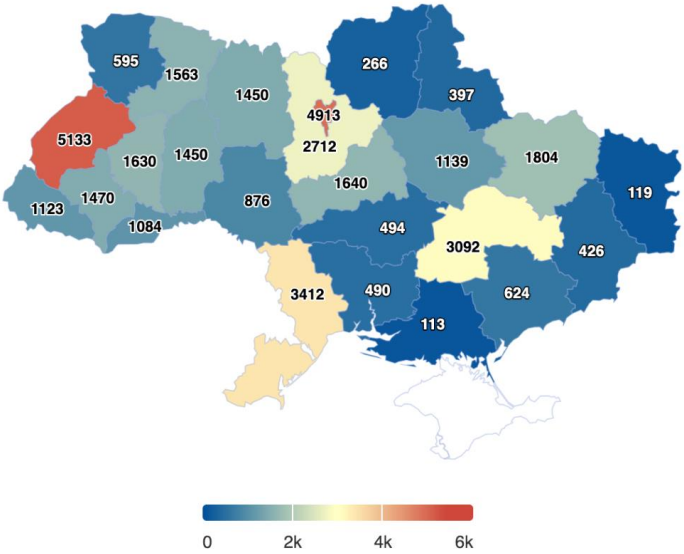

Рисунок 1 – Структура реєстрації електромобілів за регіонами на 2023 р.

Суттєвим викликом є забезпечення відповідної потужності електромереж, адже при зростанні частки електромобілів до 5–10 % від усієї парку можуть виникнути значні перевантаження на енергосистему. Це потребує реконструкції і модернізації мереж, включно з розподіленими джерелами, адаптивним навантаженням та системами розумного управління.

З розвитком ринку несуться витрати й на зарядну інфраструктуру: звичайна стаціонарна зарядка на 220 В із часом підзарядження 6–8 годин коштує 2–3 тисячі доларів, а швидкісна зарядка 400–480 В – близько 12 тисяч доларів. Станом на 2019 рік в Україні нараховувалося 2719 станцій і 5902 точки зарядки, більшість з яких підтримують стандарти Type 1, Type 2, CHAdeMO, а також CCS Combo 2). Співвідношення зареєстрованих електромобілів до точок зарядки становило

близько 4, що відповідає показникам таких країн, як Нідерланди, та перевершує Польщу [8].

Нормативно-правова база для розвитку електромобільності в Україні формувалася поступово. Закони, зокрема «Про електромобільний транспорт» 2017 року, передбачають зміни в реєстраційних правилах, встановлення технічних стандартів і безпеки, а також розвиток зарядної інфраструктури. Особливо суттєвими є податкові пільги: електромобілі звільнені від акцизного і митного зборів, ПДВ; упроваджено ставки, орієнтовані на екологічність, включно з транспортним податком і податком на нерухомість.

У 2024 році державні програми відновлення після війни були спрямовані не лише на модернізацію інфраструктури, а й на стандартизацію декарбонізації. ЄС висунув умову поєднання допомоги з дотриманням кліматичних норм; Україна впровадила програми на стимулювання електротранспорту й мереж зарядок, інтегрованих у містобудівні проєкти.

Єдиною з проблем залишається низька кількість сервісних центрів, що мають компетенцію обслуговування великих батарей, а також нестача швидких зарядних станцій уздовж автомагістралей і на АЗС. Часті технічні обмеження сумісності роз'ємів, недостатня обізнаність користувачів про роботу мобільних додатків операторів – ці чинники стримують використання електромобілів, особливо за межами великих міст [9].

Важливим пунктом є розвиток ланцюгів виробництва батарей і їх утилізації. В Україні є поклади літію (Полохівське, Станково, Шевченківське, Беганське місцезнаходження), але промислова розробка й виробництво літій-іонних батарей ще не розгорнуті системно. Натомість зростає потреба у переробці вичерпаних акумуляторів: лише близько 5% батарей у світі переробляється повторно [6]. Розвиток «другого життя» батарей для систем накопичення енергії та резервних джерел є важливим напрямом сталого розвитку. Посилення цифрової складової інфраструктури відкриває новий пласт викликів: забезпечення кібербезпеки, стандарти автентифікації, інтелектуальний моніторинг та управління зарядним процесом, сумісність обладнання різних виробників, адаптація до умов збоїв покриття мереж – усе це предмет досліджень українських інформаційних технологічних систем [7].

З глобальної перспективи, розвиток електромобільної інфраструктури в Україні тягне за собою демократизацію доступу до сталого транспорту, підвищення енергонезалежності, зниження викидів CO_2. При цьому ключовими бар'єрами залишаються відсутність чіткої реєстрації станцій, нерівномірний територіальний розвиток, технічні й фінансові бар'єри, стримування попиту. Науковці підкреслюють необхідність комплексного підходу: стимулювання попиту – через податкові пільги й муніципальні програми, нарощування пропозиції – через розвиток сервісів і зарядних мереж, модернізацію енергетичних мереж і створення нормативної бази, що включає стандарти безпеки й екологічну відповідальність.

Ураховуючи зростаючу роль електромобільного транспорту в енергетичній та транспортній системі держави, виникає об'єктивна необхідність у формуванні ефективної нормативно-правової бази, яка б регламентувала порядок їх проєктування, впровадження та експлуатації.

Нормативно-правова база захисту інформації електромобільної інфраструктури в Україні формується на базі чинного законодавства, яке визначає правові рамки відповідальності, технічних вимог та процедур контролю. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (№ 80/94-ВР) є основоположним документом, що встановлює поняття інформаційно-телекомунікаційної системи, інформує про об'єкти та суб'єктів захисту, порядок доступу, умови обробки інформації і систему відповідальності за порушення норм [10; 11]. Особливо важливо для EV-інфраструктури те, що власник системи, яким може бути оператор зарядної мережі, має обов'язок створювати службу захисту інформації або призначати відповідальних осіб і повідомляти спеціально уповноважений орган (Держспецзв'язок, CERT-UA) у разі інцидентів [10].

У табл. 1 сформовано акти, закони та постанови, які регулють діяльність та безпеку електромобільної інфраструктури. Закон «Про захист персональних даних» встановлює обов'язок збору згоди на обробку і захист персональних даних користувачів EV-інфраструктури, що стосується реєстраційних даних, платіжної інформації, історії поїздок; недотримання цих норм тягне адміністративну або кримінальну відповідальність [12]. Закон «Про критичну

інфраструктуру» поширює вимоги безпеки на об'єкти, що можуть становити загрози національній безпеці, до яких належать зарядні станції в разі критичної масовості або залучення до енергомережі високого навантаження [13].

Таблиця 1 – Нормативно-правова база захисту інформації електромобільної інфраструктури в Україні

№	Нормативний акт	Основні положення	Застосування до EV-інфраструктури
1	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР	Визначає порядок захисту інформації в ІТС, обов'язки власників, атестацію, вимоги до служб захисту	Захист інформації в зарядних системах, створення служб/відповідальних осіб
2	Закон України «Про захист персональних даних» № 2297-VI	Регламентує обробку, зберігання та захист персональних даних, згоду користувачів	Обробка даних користувачів EV-сервісів (геолокація, платежі, акаунти)
3	Закон України «Про критичну інфраструктуру» № 1647-IX	Встановлює вимоги до об'єктів критичної інфраструктури, процедури категоризації	EVSE як потенційно критичні об'єкти, потреба в оцінці ризиків
4	Указ Президента України № 695/2023	Визначає порядок реагування на загрози, взаємодію з CERT-UA, введення багаторівневого захисту	Обов'язковий моніторинг інцидентів, кіберзахист EV-мереж
5	Кодекс України про адміністративні правопорушення	Містить відповідальність за порушення вимог захисту інформації	Адміністративна відповідальність за неналежний захист інформації

Власникам EV-комплексів доведеться здійснювати категоризацію таких об'єктів, проводити оцінку ризиків, інженерний захист і забезпечувати дотримання вимог, погоджених з НАНЦ, Укренерго, Держспецзв'язком.

Указ Президента України № 695/2023 набрав чинності 17 жовтня 2023 року. Він вводить в дію рішення РНБО про захист об'єктів критичної інфраструктури та енергетики в умовах воєнних дій [14]. В цьому документі акцентовано необхідність запровадження багаторівневого захисту, посилення інженерних і кіберзасобів безпеки, взаємодії операторів інформаційно-комунікаційних систем з Центром протидії кіберзагрозам та CERT-UA, регулярного моніторингу і реагування на інциденти. EV-інфраструктура, що підпадає під цю категорію, має виконувати вимоги указу, який зобов'язує включати системи моніторингу, аудит і посилений контроль доступу до функцій керування EVSE.

EV-інфраструктура в Україні потребує дотримання щонайменше п'яти нормативних документів, що вимагають визначення об'єктів інформбезпеки, створення служб захисту, фізичного і технічного захисту, захисту персональних даних, участі у категоризації критичних об'єктів, а також інтеграції до державних структур реагування. Це дозволяє системі функціонувати в межах правового поля з чіткою відповідальністю, контролем та можливістю оперативного реагування.

Однак більшість нормативних актів не враховують специфіки функціонування зарядних станцій як об'єктів, що поєднують IT-системи, енергетичні мережі та фінансові інтерфейси. Також не врегульовано питання сертифікації ПЗ, яке використовується в EVSE, механізмів моніторингу вторгнень у реальному часі, захисту від атак на протоколи зарядки (наприклад, OCPP, ISO 15118) та прозорого розподілу відповідальності між виробниками, операторами та постачальниками цифрових рішень.

Як було зазначено, у сфері електромобільної інфраструктури зростає кількість кіберзагроз, що виникають через взаємодію між фізичними зарядними станціями, комунікаційними мережами, хмарними компонентами, мобільними додатками та основною енергосистемою. Комунікаційні канали за стандартами OCPP та ISO 15118 часто використовуються без увімкнення захисних функцій, таких як сесійне шифрування та автентифікація, що створює можливість атаки «людина-посередині», replay-атак, підробки журналів зарядок та маніпуляції з платіжними процесами [15; 16].

У статті Джонсона Дж. представлений огляд публічно зафіксованих вразливостей EVSE, що охоплюють не лише самі зарядні станції, але й комунікації зі SCADA і хмарними сервісами [15]. Типові шляхи проникнення – використання вразливих API, нешифрованих HTTP або SSH-інтерфейсів та MQTT-серверів, через які можна отримати доступ до платіжних даних або контролювати зарядку [15].

Можливості фізичного доступу через кабелі чи локальні порти дозволяють завантажувати шкідливу прошивку або проникати в локальні мережі під контролем EVSE. Так звані "juice jacking"-атаки – коли через кабель зарядки передається шкідливий код – також показують суттєвий ризик для пристроїв користувачів [16; 17].

Окремо слід виділити ризики, пов'язані з мобільними застосунками для керування зарядкою. Аналіз 31 популярного мобільного додатка виявив недостатню авторизацію користувачів або автомобілів, що дозволяє затримання сесій, нелегальний контроль процесу заряду або навіть запуск координаційних атак на енергомережу [18].

EVSE вразливі до supply-chain атак – підміни прошивки, до DoS та ботнетатак, що можуть спричинити одночасний ввімк/вимк зарядок у масштабі сотень станцій і спричинити скачки навантаження, що веде до нестабільності мережі або локальних відключень.

Нижче наведено таблицю 1 з класифікацією основних загроз та їхніх потенційних наслідків.

Загрози викликають фінансові втрати, порушення сервісу для користувачів та навіть загрожують національній безпеці через нестабільність енергосистеми. Наприклад, координовані атаки на зарядні мережі в США могли би створити навантаження, подібні до DDoS на комунікації, але спрямовані проти енергомережі. Британські та американські інфраструктури показують, що навіть несанкціоновані ремонти програмного забезпечення зарядок вже призводили до компрометації даних користувачів і порушень роботи пристроїв.

В українських умовах, із вже наявним досвідом таких подій, як атаки BlackEnergy у 2015 та Industroyer у 2016, ключовим є усвідомлення потенційних загроз EVSE. Відсутність контролю над ланцюгами постачання обладнання, слабкий сегмент мережевого розмежування та недостатній захист комунікацій створює передумови для повторення подібних сценаріїв [18; 19].

Таблиця 2 – Класифікація основних загроз та їхніх наслідків

Клас загроз	Тип атаки	Вплив
MITM / Replay	Перехоплення чи повторення пакетів OCPP/ISO 15118	Фальсифікація журналів, маніпуляція оплат
Firmware/Supply-chain	Шкідлива прошивка через кабель або порт	Блокування EVSE, мережеві проникнення
Уразливості в мобільних додатках	Захоплення сесій, ін'єкції, XSS, CSRF	Незаконний контроль EVSE, викрадення даних
DDoS/Ботнет	Масова активація/деактивація зарядок	Скачки навантаження, нестабільність мережі
Фізичний доступ	Через SSH/HTTP, USB/NFC-порти	Локальна компрометація обладнання

Системи зарядки електромобілів є складними кіберфізичними системами, які об'єднують апаратне забезпечення (зарядні станції, електромобілі), програмне забезпечення (мобільні додатки, CMS) та мережеві протоколи для обміну даними між цими компонентами. Основні функції таких систем включають ініціацію та припинення зарядних сесій, обробку платежів, моніторинг стану станцій і передачу даних про зарядку в реальному часі. Усі ці процеси залежать від надійної та безпечної передачі даних, оскільки будь-яке порушення може призвести до економічних збитків, порушення роботи інфраструктури або навіть дестабілізації електромережі.

Основними протоколами, які використовуються для передачі даних у системах зарядки електромобілів, є OCPP (Open Charge Point Protocol), ISO 15118 (Plug & Charge) та Modbus. OCPP є відкритим протоколом, який забезпечує зв'язок між зарядними станціями та CMS, дозволяючи керувати зарядними сесіями, оновлювати програмне забезпечення та обробляти платежі. ISO 15118, відомий як Plug & Charge, забезпечує автоматичну автентифікацію електромобіля та зарядної станції, що спрощує процес зарядки, але вимагає високого рівня безпеки для захисту від атак типу «людина посередині» [20]. Modbus, хоча й менш поширений, використовується для низькорівневого зв'язку в промислових системах зарядки [21]. Усі ці

протоколи потребують належного шифрування та автентифікації, щоб запобігти несанкціонованому доступу.

На рис. 2 зображено представлення протоколів передачі даних, які використовуються в процесі заряджання електромобіля.

Однією з основних загроз для систем зарядки електромобілів є атаки на мобільні додатки, які виступають інтерфейсом між користувачем і зарядною інфраструктурою.

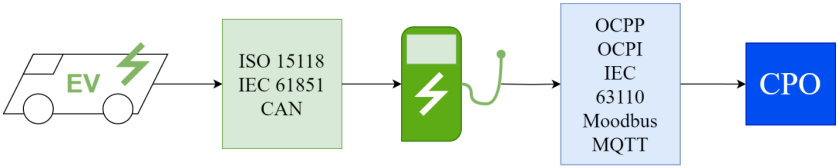

Рисунок 2 – Протоколи передачі даних у процесі зарядки

Дослідження показують, що більшість додатків вразливі через: недостатню верифікацію власності електромобіля, що дозволяє зловмисникам запускати зарядку для чужих транспортних засобів; слабку авторизацію для критичних функцій, таких як запуск і зупинка зарядки; неналежне шифрування даних, що передаються між додатком і CMS [18]. Наприклад, у реальному тесті, проведеному в 2022 році, дослідники успішно перехопили зарядні сесії в двох популярних додатках, використовуючи фальшиві акаунти [18]. В Україні такі вразливості є особливо небезпечними через обмежену кількість зарядних станцій і залежність від централізованих CMS.

Для захисту передачі даних у системах зарядки електромобілів використовуються різні технології шифрування, автентифікації та моніторингу. Найпоширенішим є протокол TLS версії 1.3, який забезпечує шифрування даних між додатком, зарядною станцією та CMS. Проте неправильна конфігурація TLS, наприклад використання застарілих версій або слабких сертифікатів, може створювати вразливості. Для підвищення безпеки також застосовується двофакторна автентифікація, яка вимагає додаткового підтвердження особи користувача, наприклад через SMS або біометричні дані. В Україні впровадження 2FA ускладнене через низький рівень цифрової грамотності користувачів і обмежену підтримку таких технологій у місцевих додатках.

Іншим важливим аспектом є верифікація власності електромобіля, яка запобігає несанкціонованим зарядним сесіям. Наприклад, протокол ISO 15118 використовує унікальний ідентифікатор транспортного засобу (VIN) для автоматичної автентифікації, що значно знижує ризик атак [20]. Однак впровадження цього протоколу в Україні обмежене через високу складність і необхідність оновлення апаратного забезпечення зарядних станцій. Альтернативним рішенням є використання фізичних ідентифікаторів, таких як RFID або QR-коди, які вимагають від користувача підтвердження присутності біля зарядної станції [18].

Масові зарядні атаки, які можуть створювати значне навантаження на електромережу, є ще однією серйозною загрозою. Дослідження на 7-шинній моделі Glover показало, що скоординована атака з використанням тисяч фальшивих акаунтів може викликати втрати до 10 % електроенергії та дестабілізацію мережі [18]. В Україні, де електромережа вже зазнає значних навантажень, такі атаки можуть мати катастрофічні наслідки. Для їх запобігання необхідні системи моніторингу в реальному часі, які виявляють аномальну активність, наприклад різке зростання кількості зарядних сесій.

Технології Vehicle-to-Grid додають додатковий рівень складності до захисту даних. V2G дозволяє електромобілям повертати енергію в мережу, що підвищує ефективність енергосистеми, але створює нові вразливості. Наприклад, скоординовані атаки на V2G-системи можуть викликати осциляторні навантаження, що призводять до коливань частоти в мережі нижче 50 Гц [22]. Для захисту V2G-систем необхідні спеціалізовані протоколи безпеки, такі як IEC 61851, які регулюють обмін даними між електромобілем і мережею.

В Україні впровадження технологій захисту даних у системах зарядки електромобілів стикається з кількома викликами. По-перше, обмежена кількість зарядних станцій і їх нерівномірний розподіл (здебільшого в містах, таких як Київ, Львів і Одеса) ускладнюють масштабування безпечних рішень. По-друге, відсутність єдиних національних стандартів безпеки для зарядної інфраструктури призводить до використання різнорідних систем, що підвищує ризик вразливостей. По-третє, низький рівень фінансування та технічної модернізації гальмує впровадження сучасних протоколів, таких як ISO 15118.

Для оцінки безпеки систем зарядки електромобілів використовуються статичні та динамічні методи аналізу. Статичний аналіз передбачає зворотне проєктування коду мобільних додатків і перевірку їхньої структури, тоді як динамічний аналіз включає моніторинг мережевого трафіку та поведінки додатків у реальному часі. В Україні такі методи рідко застосовуються через брак спеціалізованих лабораторій і експертів із кібербезпеки.

Мобільні додатки для заряджання електромобілів є частиною кіберфізичної системи, що об'єднує зарядні станції, хмарні сервери та електромобілі. Ця інтеграція створює численні вразливості, які можуть бути використані для атак. Основними вразливостями є відсутність належної верифікації власності електромобіля (Flaw 1) та неналежна авторизація для критичних функцій, таких як запуск і зупинка зарядки (Flaw 2) [18]. Ці недоліки дозволяють зловмисникам здійснювати несанкціоновані зарядні сесії, що може призвести до значних економічних і технічних наслідків.

Ключові типи атак включають:

1. Перехоплення зарядних сесій (Session Hijacking): Зловмисники можуть використовувати фальшиві акаунти для запуску зарядки електромобіля, який не належить їм, без необхідності компрометації легітимних облікових записів. Це можливо через відсутність перевірки зв'язку між користувачем і електромобілем у CMS.

2. Аналіз трафіку між додатком і CMS показав, що більшість додатків використовують HTTPS із TLS/SSL для шифрування, але вразливості в реалізації можуть дозволити перехоплення даних [23].

Координовані атаки, що використовують численні фальшиві акаунти, можуть створювати значне навантаження на електромережу, викликаючи нестабільність, як показано в симуляціях на 7-шинній моделі Glover [18].

1. Недостатня верифікація власності (Flaw 1): Більшість додатків не перевіряють, чи користувач, який ініціює зарядку, є власником електромобіля. Це дозволяє зловмисникам запускати зарядні сесії для будь-якого підключеного транспортного засобу.

2. Неналежна авторизація (Flaw 2): Критичні функції, такі як запуск і зупинка зарядки, не вимагають додаткової автентифікації, що спрощує атаки [18].

Хоча більшість додатків використовують TLS, неправильна конфігурація може призводити до вразливостей, таких як слабкі сертифікати або застарілі версії протоколів [24].

Зловмисники можуть використовувати вразливості для впливу на екосистему електромобілів. Наприклад, перехоплення зарядної сесії дозволяє зловмиснику запускати зарядку без відома власника, що може призвести до неавторизованих витрат або навіть відключення легітимного користувача від зарядної сесії. У реальному тесті, проведеному 1 листопада 2022 року, дослідники успішно перехопили зарядні сесії на двох різних додатках, підтвердивши можливість таких атак [18].

Інший сценарій передбачає масові зарядні атаки, які можуть створювати значне навантаження на електромережу. Наприклад, симуляція атаки на 7-шинну модель Glover показала, що масова зарядка може викликати втрати в передачі електроенергії та дестабілізацію мережі [18]. У сценарії, де атака розподілена пропорційно між шинами, втрати склали до 10 % від загального навантаження, що може призвести до відключення електроенергії [18].

На рис. 3 зображено схему атаки зловмисника.

Рисунок 3 – Схема атаки через мобільний додаток

Схема ілюструє, як зловмисник може ініціювати зарядку, обходячи перевірки CMS.

Атаки на мобільні додатки можуть мати серйозний вплив на електромережу, особливо в контексті технологій Vehicle-to-Grid (V2G). V2G дозволяє електромобілям повертати енергію в мережу, але вразливості в додатках можуть бути використані для створення осциляторних навантажень, що викликають коливання частоти

в мережі [25]. Наприклад, скоординована атака, що передбачає одночасне ввімкнення та вимкнення зарядки, може призвести до зниження частоти нижче 50 Гц, що вимагає відключення навантаження для стабілізації мережі.

Атака потужністю 40 кВт може викликати падіння частоти, а в поєднанні з V2G-функціями – створювати значні сплески частоти, що загрожують стабільності мережі [26].

Для зменшення вразливостей мобільних додатків в Україні необхідно впроваджувати комплексні заходи безпеки:

– Впровадження двофакторної автентифікації для критичних функцій, таких як запуск і зупинка зарядки, може значно знизити ризик несанкціонованого доступу [7].

– CMS має перевіряти зв'язок між користувачем і електромобілем, наприклад, через унікальний ідентифікатор транспортного засобу [18].

– Використання сучасних версій TLS (1.3) і регулярна перевірка сертифікатів допоможуть захистити комунікацію між додатком і CMS.

– Деякі додатки, такі як Tata Power EZ Charge, вимагають введення фізичного ідентифікатора EVCS або сканування QR-коду, що обмежує можливість віддалених атак [18].

Навчання персоналу та користувачів щодо виявлення фішингових атак і безпечного використання додатків наприклад, SMS-фішинг може бути використаний для маніпуляції поведінкою користувачів.

В Україні необхідно впроваджувати стандарти безпеки, такі як IEC 61851 та IEC 62443, які регулюють безпеку зарядних систем і кіберфізичних систем [27]. Крім того, гармонізація з європейськими стандартами, такими як GDPR, допоможе захистити персональні дані користувачів [28].

Міжнародна співпраця в цій сфері має кілька ключових переваг. По-перше, вона дозволяє Україні гармонізувати свої стандарти безпеки з міжнародними, що сприяє інтеграції до європейського цифрового ринку. По-друге, співпраця з міжнародними партнерами, зокрема в рамках ініціатив ЄС, таких як EU4Health та EU4DigitalUA, забезпечує доступ до передових технологій, фінансування та експертизи. По-третє, обмін досвідом дозволяє адаптувати глобальні

практики до локальних умов, враховуючи обмежену інфраструктуру та низький рівень цифрової грамотності в Україні.

Європейський Союз є одним із основних партнерів України в розвитку кібербезпеки, зокрема через програми EU4Health та EU4DigitalUA. EU4Health, хоча й зосереджена переважно на охороні здоров'я, включає компоненти, пов'язані з захистом критичної інфраструктури [29]. У рамках цієї програми ЄС фінансує тренінги, моделювання кібератак і розробку стратегій захисту даних, що можуть бути адаптовані до електромобільної інфраструктури. У 2021 році в Києві відбулися навчання з кібербезпеки, організовані ЄС, за участю представників Державної служби спеціального зв'язку та захисту інформації України, СБУ, Кіберполіції та інших установ [30].

EU4DigitalUA зосереджена на гармонізації цифрової інфраструктури України з Єдиним цифровим ринком ЄС. Один із її компонентів присвячений кібербезпеці та захисту даних, що включає розробку систем обміну даними, таких як «Трембіта», та впровадження стандартів захисту інформації [31]. Ці ініціативи сприяють модернізації зарядної інфраструктури через інтеграцію безпечних протоколів OCPP та ISO 15118.

В таблиці 3 наведено основні ініціативи ЄС для підтримки кібербезпеки в Україні.

Україна активно співпрацює з іншими міжнародними партнерами, такими як НАТО, США, Ізраїль та Норвегія, у сфері кібербезпеки. Наприклад, у рамках Трастового фонду Україна – НАТО з питань кібербезпеки, підписаного в 2015 році, Україна отримала програмне забезпечення, обладнання та консультативну допомогу на суму 965 млн євро [32]. Ця підтримка може бути адаптована для захисту електромобільної інфраструктури, зокрема через модернізацію дата-центрів і впровадження систем моніторингу в реальному часі.

Співпраця зі США та Ізраїлем зосереджена на залученні технологій від провідних компаній, таких як IBM, Microsoft і Radware, які розробляють рішення для захисту кіберфізичних систем [32]. Наприклад, IBM пропонує платформи на основі штучного інтелекту для виявлення аномалій у мережевому трафіку, що може бути використано для захисту зарядних станцій від масових атак [33]. Ізраїльські компанії, такі як Radware, спеціалізуються на захисті від атак типу DDoS, які можуть дестабілізувати CMS зарядних мереж.

Таблиця 3 – Ініціативи ЄС для підтримки кібербезпеки в Україні

Ініціатива	Основні цілі	Релевантність для електромобільної інфраструктури	Фінансування та період
EU4Health	Захист критичної інфраструк-тури, тренінги з кібербезпеки	Адаптація практик для захисту даних у зарядних системах	2021–2027 (5,3 млрд євро)
EU4DigitalUA	Гармонізація з цифровим ринком ЄС, розвиток систем обміну даними	Впровадження безпечних прото-колів (OCPP, ISO 15118)	2020–2025 (25 млн євро)
U-LEAD з Європою	Підтримка цифрової трансформації, навчання фахівців	Підготовка спеці-алістів для управ-ління зарядною інфраструктурою	2016–2020 (100 млн євро)

Норвегія, яка має одну з найрозвиненіших електромобільних інфраструктур у світі, може стати важливим партнером для України. Норвезький досвід впровадження стандартів ISO 15118 та технологій Vehicle-to-Grid (V2G) може бути адаптований до українських реалій, особливо для захисту даних у V2G-системах, які дозволяють електромобілям повертати енергію в мережу.

Для реалізації цих перспектив необхідно подолати виклики, пов'язані з обмеженою інфраструктурою, браком фахівців і низьким рівнем цифрової грамотності. Підвищення безпеки передачі даних у системах зарядки електромобілів в Україні зумовлене комплексними заходами, які охоплюють технічні, організаційні та регуляторні аспекти. Технічні заходи включають використання сучасних версій TLS, впровадження 2FA та верифікацію власності через VIN. Організаційні заходи передбачають навчання користувачів і персоналу щодо виявлення фішингових атак і безпечного використання додатків. Регуляторні заходи включають гармонізацію українських стандартів із міжнародними, такими як IEC 61851 та IEC 62443, а також адаптацію вимог GDPR для захисту персональних даних користувачів.

Головний напрям розвитку це розробка локалізованих рішень для України, враховуючи обмежену інфраструктуру та специфічні

виклики енергетичної системи. Наприклад, створення децентралізованих CMS може зменшити залежність від єдиних точок відмови та підвищити стійкість до атак. Крім того, необхідно інвестувати в підготовку спеціалістів із кібербезпеки, які зможуть адаптувати міжнародні практики до українських реалій.

Безпека передачі даних у системах зарядки електромобілів є критично важливою для забезпечення стабільності енергетичної інфраструктури та захисту користувачів. В Україні, де електромобільна інфраструктура активно розвивається, впровадження сучасних технологій захисту має стати пріоритетом. Водночас необхідно враховувати локальні виклики, такі як обмежена кількість зарядних станцій і низький рівень цифрової грамотності, для створення ефективних і доступних рішень.

Для впровадження змін пропонується структурований план дій, який охоплює технічні, організаційні та регуляторні заходи. На рис. 4 зображено етапи впровадження з фокусом на конкретні дії та очікувані результати.

Впровадження технологій шифрування та автентифікації спрямоване на підвищення безпеки передачі даних і доступу до систем електромобільної інфраструктури.

Необхідно налаштувати протокол Transport Layer Security версії 1.3 для всіх каналів зв'язку, включаючи комунікацію між мобільними додатками, системами керування зарядкою і зарядними станціями.

Це передбачає оновлення серверного програмного забезпечення, встановлення надійних сертифікатів і регулярну перевірку їхньої актуальності для запобігання використанню застарілих або слабких сертифікатів, які можуть бути вразливими до атак типу «людина посередині».

Паралельно впроваджується двофакторна автентифікація для критичних функцій, таких як запуск і зупинка зарядних сесій, використовуючи підтвердження через SMS, біометричні дані (наприклад, сканування відбитків пальців) або сканування QR-кодів на зарядній станції, щоб знизити ризик несанкціонованого доступу, навіть якщо зловмисники отримають доступ до облікових даних користувача.

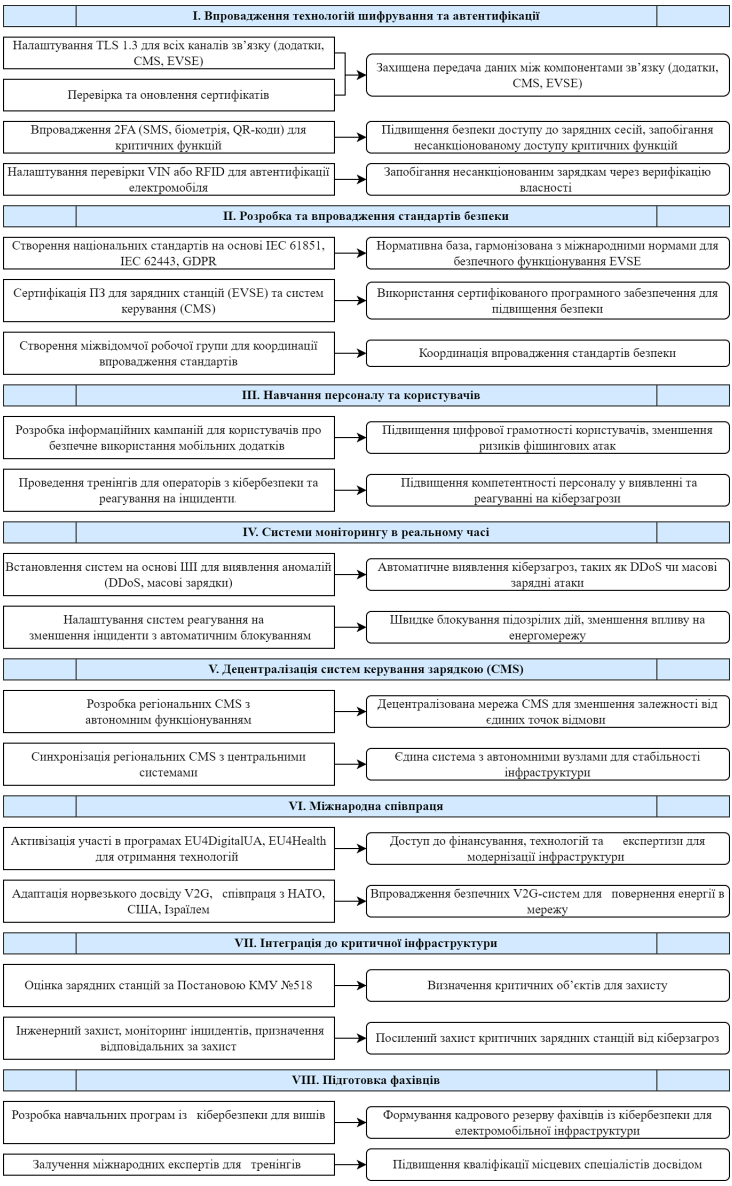

Рисунок 4 – Етапи впровадження змін до захисту інформації в процесі функціонування електромобільної інфраструктури в Україні

Також налаштовується верифікація власності електромобіля через унікальний ідентифікатор транспортного засобу або фізичні ідентифікатори, такі як RFID-мітки, що забезпечить можливість ініціювання зарядки лише власником або авторизованим користувачем, зменшуючи ризик атак типу “session hijacking”.

За реалізацію відповідають оператори зарядних мереж, розробники програмного забезпечення та виробники зарядних станцій, які співпрацюють для оновлення апаратного й програмного забезпечення з метою підтримки цих функцій. Очікувані результати включають захищену передачу даних між компонентами інфраструктури, підвищення безпеки доступу до зарядних сесій і запобігання несанкціонованим зарядкам.

На цьому етапі розробки та впровадження стандартів безпеки створюється регуляторна база для забезпечення безпеки електромобільної інфраструктури. Розробляються національні стандарти безпеки, гармонізовані з міжнародними нормами, такими як IEC 61851 (для систем зарядки електромобілів), IEC 62443 (для безпеки кіберфізичних систем) і GDPR (для захисту персональних даних), які визначатимуть вимоги до шифрування, автентифікації, моніторингу та обробки даних користувачів, включаючи геолокацію, платіжну інформацію та історію зарядок. Проводиться сертифікація програмного забезпечення для зарядних станцій і систем керування зарядкою на відповідність стандартам безпеки, зокрема захист від вразливостей, таких як слабке шифрування чи недостатня авторизація. Для координації впровадження стандартів створюється міжвідомча робоча група за участю Міністерства інфраструктури, Держспецзв’язку та операторів зарядних мереж, яка забезпечує обмін інформацією між зацікавленими сторонами та контролює дотримання вимог. Відповідальність за розробку стандартів і координацію покладається на Міністерство інфраструктури та Держспецзв’язок, тоді як сертифікацію проводять спеціалізовані центри за участю операторів мереж.

Етап навчання персоналу та користувачів зосереджений на підвищенні рівня безпеки через підготовку операторів зарядних мереж і користувачів електромобілів. Проводяться регулярні тренінги для персоналу операторів із питань кібербезпеки, які охоплюють

виявлення фішингових атак, налаштування безпечного обладнання, реагування на кіберінциденти та використання систем моніторингу. Організацію тренінгів забезпечують оператори мереж у співпраці з громадськими організаціями, які мають досвід у сфері кібербезпеки. Водночас розробляються інформаційні кампанії для користувачів електромобілів, спрямовані на підвищення цифрової грамотності, що пояснюють, як безпечно використовувати мобільні додатки, уникати атак типу "juice jacking" (передача шкідливого коду через зарядні кабелі) і розпізнавати SMS-фішинг. Для цього оператори мереж співпрацюють із медіа та громадськими організаціями, створюючи доступні матеріали, такі як відео, інфографіки чи посібники.

На етапі системи моніторингу створюється інфраструктура для виявлення та реагування на кіберзагрози. Встановлюються системи на основі штучного інтелекту для моніторингу аномальної активності, такої як DDoS-атаки чи масові зарядні атаки, які можуть дестабілізувати електромережу. Ці системи аналізують мережевий трафік і поведінку зарядних сесій, виявляючи підозрілі дії, наприклад, різке зростання кількості одночасних зарядок. Впровадження забезпечують оператори зарядних мереж у співпраці з CERT-UA та IT-компаніями, такими як IBM чи Radware, які надають рішення для захисту кіберфізичних систем. Налаштовуються системи автоматичного реагування на інциденти, які блокують підозрілі дії, наприклад, несанкціоновані зарядні сесії чи спроби доступу до CMS, із інтеграцією до центральних платформ моніторингу. За це відповідають CERT-UA та оператори мереж.

Для підвищення стійкості до атак децентралізуються системи керування зарядкою. Розробляються регіональні CMS, які працюють автономно, але синхронізуються з центральними системами для обміну даними, наприклад, про стан зарядних станцій чи історію транзакцій. Це зменшує залежність від єдиних точок відмови, таких як централізовані сервери, і забезпечує стабільність у разі збоїв мережі. Оператори зарядних мереж і Укренерго відповідають за проєктування та тестування регіональних CMS, тоді як розробники програмного забезпечення та оператори мереж забезпечують сумісність і безпеку зв'язку між регіональними та центральними системами.

Міжнародна співпраця необхідна для отримання технологій, фінансування та експертизи. Активізується участь України в програмах ЄС, таких як EU4DigitalUA та EU4Health, які надають ресурси для розвитку кібербезпеки та цифрової інфраструктури. Мінцифри, МЗС і оператори зарядних мереж координують участь у цих програмах, адаптуючи європейські практики до локальних умов. Співпраця з партнерами, такими як Норвегія, НАТО, США та Ізраїль, дозволяє впроваджувати передові рішення, зокрема технології Vehicle-to-Grid, використовуючи норвезький досвід для налаштування безпечних V2G-систем, які дозволяють електромобілям повертати енергію в мережу. Мінцифри та оператори мереж співпрацюють із міжнародними компаніями, такими як IBM і Radware, для інтеграції їхніх рішень.

Етап інтеграції передбачає включення зарядних станцій до об'єктів критичної інфраструктури. Проводиться категоризація зарядних станцій відповідно до Постанови КМУ № 518, оцінюючи їхню важливість для енергосистеми та потенційні ризики в разі атак. Впроваджується інженерний захист, моніторинг інцидентів і призначення відповідальних осіб для управління безпекою, включаючи обмеження доступу до портів USB чи NFC і підключення до систем моніторингу CERT-UA. Оператори мереж, CERT-UA і Укренерго відповідають за оцінку та захист, а Держспецзв'язок забезпечує дотримання вимог.

Підготовка фахівців зосереджена на формуванні кадрового резерву. Розробляються навчальні програми з кібербезпеки для вищих навчальних закладів, які готуватимуть спеціалістів із захисту електромобільної інфраструктури. ВНЗ співпрацюють із міжнародними партнерами, такими як ЄС чи НАТО, для створення актуальних курсів. Залучаються міжнародні експерти для проведення тренінгів із сучасних технологій захисту, таких як моніторинг аномалій чи захист V2G-систем. Мінцифри та ВНЗ координують ці програми, залучаючи фінансування через міжнародні гранти.

Ці етапи забезпечать комплексний захист інформації в електромобільній інфраструктурі, підвищать її стійкість до кіберзагроз і сприятимуть інтеграції з європейськими стандартами, враховуючи локальні виклики, такі як обмежена інфраструктура та низька цифрова грамотність.

Висновки. Розвиток електромобільної інфраструктури в Україні є ключовим елементом переходу до сталого транспорту, декарбонізації та енергетичної незалежності, проте супроводжується значними викликами у сфері захисту інформації. Електромобільна інфраструктура, як кіберфізична система, об'єднує зарядні станції, системи керування зарядкою, мобільні додатки та енергомережі, що створює численні вразливості до кіберзагроз, таких як атаки типу «людина посередині», перехоплення зарядних сесій, DDoS-атаки та маніпуляції з платіжними даними. Відсутність єдиних національних стандартів безпеки, недостатня верифікація власності електромобілів і слабке шифрування в протоколах OCPP та ISO 15118 підвищують ризики для безпеки користувачів і стабільності енергосистеми. В Україні ці проблеми ускладнюються обмеженою кількістю зарядних станцій, нерівномірним їх розподілом, низьким рівнем цифрової грамотності та нестачею фахівців із кібербезпеки. Нормативно-правова база, включаючи закони про захист інформації, персональних даних і критичну інфраструктуру, частково регулює діяльність електромобільної інфраструктури, але не враховує її специфіки, зокрема унікальних вимог до захисту кіберфізичних систем і сертифікації програмного забезпечення. Впровадження комплексних заходів, таких як використання протоколу TLS 1.3, двофакторної автентифікації, верифікації через VIN або RFID, децентралізації систем керування зарядкою та моніторингу в реальному часі на основі штучного інтелекту, може значно підвищити безпеку. Міжнародна співпраця, зокрема через програми ЄС та партнерство з Норвегією, НАТО, США й Ізраїлем, забезпечує доступ до технологій, фінансування та експертизи, що дозволяє адаптувати передові практики до локальних умов. Гармонізація з міжнародними стандартами сприятиме захисту даних і підвищенню довіри користувачів. Навчання персоналу та користувачів, а також підготовка фахівців із кібербезпеки через спеціалізовані програми у вишах, є критично важливими для подолання кадрового дефіциту та підвищення цифрової грамотності. Інтеграція зарядних станцій до об'єктів критичної інфраструктури з дотриманням вимог забезпечить їхній захист від загроз національній безпеці. Таким чином, комплексний підхід, що поєднує технічні, організаційні та

регуляторні заходи, дозволить Україні створити стійку та безпечну електромобільну інфраструктуру, яка відповідає сучасним викликам і сприяє сталому розвитку, енергетичній стабільності та інтеграції до європейського цифрового простору.

Список використаних джерел

1. Алімурадов Ш. Р. Електромобільна інфраструктура як об'єкт дослідження транспортної логістики. *Вісник Одеського національного морського університету*. 2021. № 67. С. 104–110.
2. Tamay P., Inga Ortega E. Charging Infrastructure for Electric Vehicles Considering Their Integration into the Smart Grid. *Sustainability*. 2022. Vol. 14. P. 8248–8267. DOI: 10.3390/su14148248
3. Ajanovic A., Haas R. Dissemination of electric vehicles in urban areas: major factors for success. *Energy*. 2016. Vol. 115. P. 1451–1458.
4. Zhang X., Xie J., Rao R., Liang Y. Policy incentives for the adoption of electric vehicles across countries. *Sustainability.* 2020. Vol. 12 (10). P. 4321.
5. Zharovska I., Kozak Y., Semenov V. Comprehensive study on electric vehicles and infrastructure for sustainable development in Ukraine. *Energies.* 2023. Vol. 16 (7). DOI: https://doi.org/10.1051/e3sconf/202456701025
6. Pivnyak G., Olishevska V., Olishevskiy H., Lutsenko I., Lysenko A. Comprehensive study on electric vehicles and infrastructure for sustainable development in Ukraine. *E3S Web of Conferences*. 2024. DOI: 10.1051/e3sconf/202456701025
7. Марків О., Ришковець Ю. Інформаційні технології і протоколи передачі даних у системах зарядки електромобілів. *Information Systems and Networks*. 2025. Вип. 17. С. 304–318. DOI: https://doi.org/10.23939/sisn2025.17.304.
8. Грома Я. В., Глущенко Я. І. Порівняльний аналіз ринку електромобілів в Україні та світі. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут»*. 2019. № 16. С. 42–49.
9. Чорний Р. С., Чорна Н. П., Шевчук Я. В. Електромобільна інфраструктура в Україні: проблеми та перспективи розвитку. *Міжнародний науковий журнал Інтернаука.* 2020. № 19 (2). С. 49–53.

10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 20.04.2025. *Верховна рада.* URL: https://zakon.rada.gov.ua/go/80/94-вр

11. Кодекс України про адміністративні правопорушення : щодо відповідальності за недотримання умов захисту інформації. *Відомості Верховної Ради Української РСР* (ВВР) 1984, додаток до № 51, ст.1122) URL: https://dduvs.edu.ua/wp-content/uploads/files/Structure/f/fpfpmgb/p/d3.pdf

12. Про захист персональних даних : Закон України від від 23.02.2012 р. № № 4452-VI. Дата оновлення: 14.06.2025. *Верховна рада України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

13. Про критичну інфраструктуру : Закон України від від 18.11.2021 р. № 1909-IX. Дата оновлення: 21.09.2024. *Верховна рада України.* URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

14. Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій : Указ Президента України від 17.10.2023 р. № 695/2023. Дата оновлення: 19.10.2023. *Верховна рада України.* URL: https://zakon.rada.gov.ua/laws/show/n0040525-23#Text

15. Johnson J., Berg T., Anderson B., Wright B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies*. 2022. Vol. 15 (11). P. 3931–3952. DOI: 10.3390/en15113931

16. Poudel S., Baugh J. E., Takiddin A., Ismail M., Refaat S. S. Injection attacks and detection strategy in front-end vehicle-to-grid communication. *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. Glasgow, United Kingdom. 2023. P. 1–6. DOI: 10.1109/SmartGridComm57358.2023.10333927

17. Nasr T., Torabi S., Bou-Harb E. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security*. 2022. Vol. 112. P. 102511. DOI: 10.1016/j.cose.2021.102511

18. Sarieddine K., Sayed M. A., Torabi S. та ін. Investigating the Security of EV Charging Mobile Applications As an Attack Surface. *arXiv*. 2022. URL: https://arxiv.org/abs/2211.10603

19. Yemelyanov V., Bondar H. Cyber security as a component of national security and cyber protection of critical infrastructure of Ukraine. *Public Administration and Regional Development.* 2019. № 5. P. 493–523. DOI: 10.34132/pard2019.05.02

20. Attanasio L., Conti M., Donadel D., Turrin F. MiniV2G: an electric vehicle charging emulator. *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*. 2021. P. 65–73.

21. Alzahrani A., Wangikar S. M., Indragandhi V., Singh R. R., Subramaniyaswamy V. Design and implementation of SAE J1939 and Modbus communication protocols for electric vehicle. *Machines*. 2023. Vol. 11 (2). P. 201–223. DOI: https://doi.org/10.3390/machines11020201

22. Chen G., Zhang Z. Control Strategies, Economic Benefits, and Challenges of Vehicle-to-Grid Applications: Recent Trends Research. *World Electric Vehicle Journal.* 2024. Vol. 15 (5). P. 190–214. DOI: 10.3390/wevj15050190

23. Van Aubel P., Poll E. Security of EV-charging protocols. *arXiv*. 2022. URL: https://arxiv.org/abs/2202.04631

24. Sarieddine K., Sayed M. A., Assi C., Atallah R., Torabi S., Khoury J. EV charging infrastructure discovery to contextualize its deployment security. *IEEE Transactions on Network and Service Management*. 2023. Vol. 21 (1). P. 1287–1301. DOI: 10.1109/TNSM.2023.3318406

25. Johnson J. & et. Cybersecurity for Electric Vehicle Charging Infrastructure. *SANDIA REPORT*. 2022. 66 p. DOI: 10.2172/1877784

26. Sayed M. A., Ghafouri M., Atallah R., Debbabi M., Assi C. An Electric Vehicle Control Strategy to Mitigate Load Altering Attacks Against Power Grids. *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE).* 2023. P. 1–6. DOI: 10.1109/ICRAIE59459.2023.10468152

27. ДСТУ EN IEC 61851-1:2021. Система зарядки електричних транспортних засобів дротова. Частина 1. *Загальні вимоги.* URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=95965

28. General Data Protection Regulation (GDPR). *Official Journal of the European Union.* 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

29. EU4Health Programme. *European Commission*. 2021. URL: https://ec.europa.eu/health/funding/eu4health_en

30. EU enhances Ukraine's capacity to respond to cyber-attacks. Офіційний вебсайт. URL: https://eufordigital.eu/eu-enhances-ukraines-capacity-to-respond-to-cyberattacks/

31. EU4DigitalUA: Interoperability, E-services and Cybersecurity for Ukraine. *e-Governance Academy.* 2020. URL: https://ega.ee/project/eu4digitalua/.

32. Український кіберпростір: безпекові загрози, виклики та перспективи розвитку. *Аналітичний центр ADASTRA*. 2020. URL: https://adastra.org.ua/blog/ukrayinskij-kiberprostir-bezpekovi-zagrozi-vikliki-ta-perspektivi-rozvitku.

33. IBM Security.IBM. Офіційний сайт. 2025. URL: https://www.ibm.com/security.