УДК. 629.02

DOI: 10.33868/0365-8392-2025-1-282-2-7

© П. В. Кисловський, заступник завідувача відділу,
ORCID: 0000-0001-8495-7130,
e-mail: pkyslovskyy@insat.org.ua
(ДП «ДержавтотрансНДІпроект»);
© М. М. Ященко, канд. техн. наук, доцент,
ORCID: 0000-0003-2418-1910,
e-mail: nikyaschenko@gmail.com,
(Національний транспортний університет);
© В. М. Ященко, інженер,
ORCID: 0000-0002-3501-6227,
e-mail: vyashchenko@insat.org.ua
(ДП «ДержавтотрансНДІпроект»)

© Petro Kyslovskyi, Deputy Head of Division,
ORCID: 0000-0001-8495-7130,
e-mail: pkyslovskyy@insat.org.ua
(State Road Transport Research Institute);
©Mykola Yashchenko, Ph.D.,
ORCID: 0000-0003-2418-1910,
e-mail: nikyaschenko@gmail.com
(National Transport University);
© Valentyn Yashchenko, Engineer,
ORCID: 0000-0002-3501-6227,
e-mail: vyashchenko@insat.org.ua
(State Road Transport Research Institute)

КІБЕРБЕЗПЕКА ЕЛЕКТРОМОБІЛІВ ТА ЇХНІХ ЗАРЯДНИХ ПРИСТРОЇВ

CYBERSECURITY OF ELECTRIC VEHICLES AND CHARGING SYSTEMS

Анотація. *Розглянуто основи роботи комунікаційних систем електромобіля і чинники, що впливають на їхню безпеку. Обґрунтовується використання нових правил щодо стійкості шифрування засобів зв'язку електромобіля та їхні основні недоліки, що можуть призвести до витоку конфіденційної інформації. Оцінюється вплив автовиробників на створення єдиних систем і протоколів щодо взаємодії між електромобілями та зарядною інфраструктурою. Пропонується переглянути стандарти для електромобілів, що підвищить їхню кібербезпеку як єдиної системи, підключеної до споживчих мобільних пристроїв і зарядних станцій.*

Ключові слова*: електромобіль, зарядна інфраструктура, інтерфейс, комунікаційний стандарт, відкритий протокол заряджання, інфраструктура відкритих ключів, кібербезпека електромобіля.*

Abstract*. The article shows the basics of communication systems for electric vehicles and charging systems and factors affecting their safety. Electric vehicle has a number of systems for data exchange between electronic control units of the vehicle. This unit's exchange signals, which can be used by hackers to access information through the interfaces that are in the electric vehicle. Charging systems also poses risks to confidential information through unauthorized access to a charging unit. Potential vulnerabilities that can be exploited in case of insufficient protection or charging station are: the combination of short data encryption keys and long periods of their validity; insufficient use of encryption algorithms; using outdated cryptographic algorithms. To increase the safety of the charging infrastructure it: must support the remote change of all passwords; must be able to use certificates issued by the Public Key Infrastructure (PKI); should detect physical tampering by having a cover; must have sufficient memory and processing power. However, the question of information transfer between the electric vehicle and the charging equipment has not been treated sufficiently. Such communication is necessary for the optimization of energy resources and energy production systems so that vehicles can recharge in the most economical and most safely way. It is proposed to review the standards for electric vehicles, which will increase their cyber security as a single system connected to consumers of mobile devices and charging stations. The new communication standard may serve in the future to contribute to the stabilization of the electrical grid as well as to support additional information services required to operate electric vehicles efficiently and economically.*

Keywords*: electric vehicle, charging infrastructure, charging interfaces, communication standards, open charge point protocol, public key infrastructure, cybersecurity.*

Вступ

Збільшення кількості електромобілів на дорогах вимагає ретельного аналізу безпеки як транспортних засобів, так і зарядної інфраструктури. Електромобілі оснащені багатьма електронними блоками керування, датчиками і механізмами, що контролюють системи транспортних засобів. Кожен електронний блок відповідає за керування механічними або електричними компонентами сучасного електромобіля. Значна частина зв'язку між блоками відбувається через мережу Controller Area Network (CAN). Крім того, блок керування комунікаціями (TCU) надсилає діагностичну інформацію виробнику оригінального обладнання електромобіля. Сучасні електромобілі зазвичай оснащені WiFi, Bluetooth, 4G/5G та іншими видами бездротового зв'язку. Усі перелічені інтерфейси і мережі зв'язку потенційно дозволяють зловмисникам впливати на безпечну роботу транспортного засобу та на його власника.

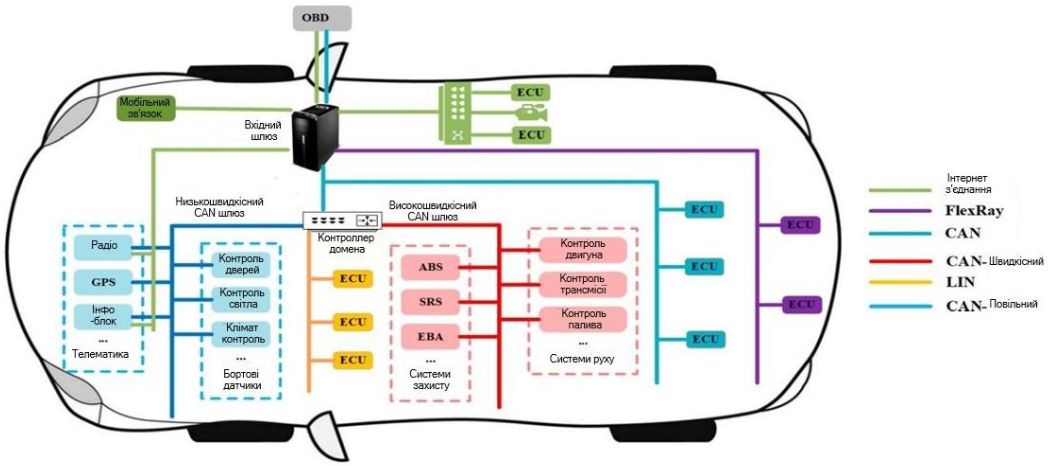

Рис. 1. Види мереж для зв'язку між блоками керування електромобіля

Безпечне заряджання електромобіля також є серйозною проблемою, що пов'язано з різними характеристиками під'єднання, системами авторизації та відмінностями засобів безпеки зарядних пристроїв від різних виробників. Через високу конкуренцію за споживача технічні можливості зарядних пристроїв балансують між функціональністю та сумісністю, вартістю і безпекою.

Подальший розвиток та ускладнення конструкції електромобілів породжують усе нові й нові загрози їхньої безпечної експлуатації. Тому особливу увагу необхідно приділяти безпечній та надійній комунікації електронних засобів електромобіля з навколишнім середовищем. За Правилами № 155 ЄЕК ООН кібербезпека електромобіля – це стан, у якому він та його функції захищені від кіберзагроз, яким можуть піддаватися електричні або електронні компоненти [1].

Основна частина

Для розуміння основних напрямів атаки хакерів необхідно розглянути структуру зв'язку між електронними системами електромобіля, а також їхню електронну взаємодію із зарядними пристроями.

Наслідки атак можуть бути досить руйнівними і за Правилами № 155 ЄЕК ООН охоплюють:

- порушення безпечної роботи або відмову від деяких функцій транспортного засобу;
- модифікацію програмного забезпечення зі зниженням його ефективності;
- порушення цілісності та конфіденційності даних;
- втрату можливості виведення даних;
- інші наслідки, зокрема злочинні дії [1].

Основний зв'язок між блоками керування електромобіля проходить через дроти електронного блока управління ECU (Electronic Control Unit), що з'єднують його компоненти. Цей зв'язок реалізується через мережу контролера CAN (Controller Area Network) і локальну міжсистемну мережу LIN (Local Interconnect Network). CAN є основною мережею електромобіля, яка дозволяє здійснювати швидкісний зв'язок, самодіагностику і виправлення помилок. Мережа LIN є доповненням до мережі CAN. Вона з'єднує між собою меншу кількість блоків керування і пропонує дешевшу реалізацію завдяки нижчій продуктивності та надійності. Мережа LIN може використовуватися для керування двигуном, трансмісією, датчиками і приводами гальм і коліс, кондиціонером, дверима і сидіннями.

Сучасні електромобілі також містять механізми оновлення внутрішнього програмного забезпечення. Ця послуга зазвичай реалізується за допомогою роз'єму зовнішнього пристрою USB або через бездротове підключення до Інтернету. Крім того, сучасний електромобіль має розважальні системи, що можуть розширити можливості небезпечного підключення.

Електромобілі мають, в основному, ту саму побудову, що і транспортні засоби з ДВЗ. Але вони також містять компоненти, що керують зберіганням та накопиченням електроенергії,

генерують електроенергію і виконують рух коліс.

Акумулятор забезпечує потужність, необхідну для роботи компонентів електромобіля. Система керування акумулятором (BMS) регулює вихідний струм, а також заряджання і розряджання акумулятора, зберігаючи його в безпечній робочій зоні. BMS контролює всю батарею в комплекті і вимірює напругу, струм і температуру кожної комірки батареї. Вона має можливості для обмеження напруги для кожної з комірок, у разі, якщо значення перевищують порогові. BMS також вимірює стан заряду і працездатність акумулятора.

Зарядна система перетворює вхідну напругу на постійний струм і передає її на акумулятор для зберігання.

Крім того, вона запобігає можливим пошкодженням батареї або системи живлення, обмежуючи потік електроенергії.

Контролер (CAN) регулює потік струму від батареї до систем електромобіля, отримуючи вхідні дані від водія для керування прискоренням, гальмуванням, режимом водіння і перетворює енергію батареї з постійного струму на змінний.

Всі згадані компоненти повинні обмінюватися повідомленнями між собою, щоб гарантувати правильну роботу електромобіля, що потенційно розширює можливості небезпечного підключення ззовні [2].

Зарядна інфраструктура для електромобіля використовує подібні мережі для заряджання акумулятора, зокрема бездротовим способом. Основними вимогами щодо кібербезпеки зарядної станції є:

- зарядна станція повинна підтримувати дистанційну зміну всіх паролів і ключів, щоб захистити їхню конфіденційність і цілісність;

- використовуючи сертифікати для автентифікації або безпеки зв'язку, зарядна станція повинна мати можливість застосовувати сертифікати, видані інфраструктурою відкритих ключів (PKI) (англ. public key infrastructure);

- зарядна станція повинна мати спеціальну кришку для захисту від фізичного втручання, щоб зловмисники без спеціальних інструментів не змогли дістатися до її електронних компонентів, не залишивши видимих слідів;

- зарядна станція повинна мати достатню кількість пам'яті (RAM та флеш-пам'ять), а також обчислювальну потужність, щоб забезпечити встановлення оновлень безпеки, необхідних протягом усього терміну служби [3].

У процесі дротового заряджання зарядний пристрій обмінюється із зарядною станцією контрольними сигналами, які містять інформацію щодо ємності акумулятора і потужності електромережі.

Зарядні пристрої зі змінним струмом мають низьку потужність і не потребують мереж зв'язку, оскільки не використовують керування напругою. У зарядних пристроях із постійним струмом використовуються розширені можливості управління напругою, що забезпечують мережі CAN або Power Line Communication (PLC). Ці мережі також дозволяють автоматизувати процес виставлення рахунків і завантаження оновлень програмного забезпечення пристрою.

Однофазні зарядні пристрої застосовують п'ятививідний роз'єм, що має вигляд зарядного пристрою типу SAE J1772 або IEC 62196. Цей роз'єм використовує два дроти для передачі зарядного струму, два – для передачі сигналів і один – для заземлення [4].

Два дроти для сигналів призначені для обміну інформацією з електромобілем під час сеансу заряджання. Сигнали контролюють величину струму, що подається до електромобіля, або використовуються для перевірки стану під'єднання і припинення живлення в разі неналежного фізичного з'єднання із зарядним пристроєм.

Зарядні пристрої, що дозволяють швидке заряджання електромобіля, мають кілька видів. Перший – це модифікація Combined Charging System (CCS) для зарядного пристрою типу SAE J1772 або IEC 62196, який дозволяє заряджатися постійним струмом. Цей вид зарядного пристрою використовує мережу PLC для обміну додатковою інформацією з електромобілем. Другий вид – зарядний пристрій CHAdeMO, який також забезпечує швидке заряджання. Окрім живлення, він дає змогу обмінюватися додатковою інформацією через мережу CAN. Крім того, зарядний пристрій CHAdeMO забезпечує зв'язок Vehicle to Grid, який передбачає використання акумулятора електромобіля як накопичувача енергії для передачі до електромережі під час стоянки. У США для електромобілів Tesla використовують власний, несумісний з іншими видами зарядний пристрій. У КНР використовується

пристрій Chaoji, який є сумісним із видами CCS і CHAdeMO.

Структура надання послуг зарядних станцій передбачає створення окремих операторів галузі. Оператор енергомережі передає напругу до зарядної станції. Оператор зарядної станції – це компанія, яка відповідає за встановлення, управління та обслуговування зарядних станцій. Постачальник послуг у сфері мобільності – це організація, яка надає кінцевому споживачу послуги для пошуку зарядних станцій, ідентифікації споживача та оплати сеансу заряджання, укладаючи договір із водієм електромобіля.

Протокол Open Smart Charging Protocol (OSCP) забезпечує обмін даними між оператором енергомережі та оператором зарядних станцій.

Відповідно, протокол Open Charge Point Interface (OCPI) використовується для обміну даними між оператором зарядної станції та постачальником послуг у сфері мобільності, а також з іншими операторами ринку, яким потрібна інформація про електромобіль. Також протокол OCPI призначений для обміну даними про локації, тарифи, дозволи та операції з оплати заряджання.

Водночас зв'язок електромобіля та зарядної станції передбачає застосування протоколів Open Charge Point Protocol (OCPP) або ISO 15118, які використовують відповідні сертифікати. Для з'єднання користувач електромобіля застосовує кабель, і електромобіль надсилає сертифікати, яким він довіряє. Зарядна станція вибирає один зі своїх сертифікатів і використовує його для початку з'єднання Transport Layer Security (TLS), тобто для криптографічного шифрування. TLS охоплює три основні фази: діалог між сторонами, метою якого є вибір алгоритму шифрування; обмін ключами на основі криптосистем із відкритим ключем; передача даних. Далі електромобіль запитує доказ, що сертифікат зарядної станції все ще дійсний. На перший погляд всі ці операції з алгоритмом шифрування та ключами надійно захищають зв'язок електромобіля та зарядної станції, але, з іншого боку, кожна з них потенційно збільшує ризик несанкціонованого підключення під час заряджання.

Будь-який зарядний пристрій має зв'язок із постачальником послуг задля відстеження сеансів заряджання і збору даних. Найбільш поширеними для використання в галузі є протоколи OCPP та IEEE 2030.5, але існують й інші види протоколів. Вони застосовують сертифікати для налаштування з'єднання TLS, яке дозволяє захистити клієнт-серверні додатки від перехоплення, редагування або створення підроблених повідомлень. Для взаємної автентифікації кожна зі сторін мусить підтримувати інфраструктуру відкритих ключів PKI.

Технологія PKI полягає у використанні двох математично пов'язаних цифрових ключів, що мають таку властивість: один ключ може бути використаний для шифрування з'єднання, яке може бути розшифровано тільки за допомогою другого ключа. Навіть якщо відомий один ключ, за допомогою обчислень практично неможливо визначити другий. Тут діє принцип банківської комірки – один із ключів відкритий для всіх, а інший має приватний характер і зберігається в захищеному місці. Інфраструктура відкритих ключів передбачає, що сторони в обміні даними покладаються на центри сертифікації. Поки що не створено єдиного органу зі зберігання ключів, але над проблемою працюють такі автомобільні концерни, як BMW AG, Groupe Renault, Porsche AG, Stellantis, Volkswagen AG.

Основний варіант для побудови структури PKI полягає в тому, щоб мати лише один довірений сертифікат, яким керує учасник ринку, галузева асоціація або нейтральна організація державного рівня. Зараз уже існує кілька незалежних PKI. Технічно найпростіший спосіб досягнення сумісності різних структур PKI передбачає розпізнавання електромобілем усіх довірених сертифікатів як надійних. Це означає, що всі електромобілі мають зберігати всі сертифікати у своєму сховищі, як і всі зарядні станції.

Головною перевагою, яка й забезпечила нинішню популярність протоколу OCPP серед інших протоколів зв'язку, є те, що це відкритий для розробників і користувачів, а також безкоштовний протокол. Проте він має низку недоліків, серед яких:

- перевірка великої кількості сертифікатів займає багато часу, оскільки пам'ять пристрою, потужність обробки та пропускна здатність зв'язку обмежені;

- інформація, що передається за допомогою OCPP, може бути атакована способом перехоплення електромагнітного випромінювання під час використання мережі PLC зарядним пристроєм;

- сьогодні все ще використовують попередні версії протоколу OCPP, а багато наявних зарядних пристроїв покладаються на старіші версії протоколу, ніж версія 2.0.

Окрім цього, навіть для OCPP 2.0 зв'язок TLS не є обов'язковим, оскільки передбачено два види авторизації: в першому випадку оператор послуг і зарядна станція з'єднуються за допомогою мережевого протоколу HTTP з використанням пароля; у другому з'єднання відбувається за допомогою TLS і довіреного сертифіката. Навіть якщо зарядний пристрій застосовує останню версію протоколу OCPP, необхідно віддавати перевагу найновішим версіям TLS, оскільки за умови використання версій нижче за 1.2 рівень кібербезпеки є надто низьким.

З метою покращення взаємодії з клієнтом у разі заряджання через зарядний пристрій CCS була розроблена функція «plug-and-charge» (англ. «підключай і заряджай»). Вона дозволяє автоматизувати процеси зв'язку та виставлення рахунків між електромобілем і зарядною станцією без використання карток RFID або додатків для заряджання, водночас забезпечуючи високу кі-бербезпеку.

Широкому впровадженню «plug-and-charge» заважає відсутність не лише консенсусу серед виробників автомобільної галузі, а й стандартизації зарядних пристроїв та комунікаційних протоколів. Технологія «plug-and-charge», яка доступна за стандартом ISO 15118-2 (за умови оновлення програмного забезпечення електромобіля) або ISO 15118-20 («Інтерфейс зв'язку транспортного засобу з мережею», опубліковано 2022 року) дозволяє автоматично авторизуватись електромобілю за допомогою технології відкритих ключів (PKI) та унікально ідентифікує кожен електромобіль [5].

Уряд Німеччини вже зробив стандарт ISO 15118-20 невід'ємною частиною запланованої програми субсидій для громадської звичайної та швидкої зарядної інфраструктури, щоб побудувати зарядні станції, обладнані для майбутнього використання. Штат Каліфорнія (США) зазначив, що вимоги цього стандарту мають застосовуватись до всіх зарядних станцій [6].

Уряд Британії вживає заходів для стимулювання цього переходу, щоб усі зарядні точки, які продаються чи встановлюються в країні, мали розумні функції. Тому Велика Британія розробила свій власний стандарт PAS 1899:2022 на основі вже чинних стандартів [7]:

- OCPP, який передбачає зв'язок між зарядними станціями та оператором послуг;
- ISO 15118-20, який визначає спосіб зв'язку між електромобілем і зарядною інфраструктурою;
- EE Bus IoT, що є стандартом сумісності;
- IEC 63110, який визначає протокол для керування інфраструктурою зарядки транспортних засобів;
- Open ADR, що є стандартом управління енергією;
- ISO/IEC 27001:2022 – «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги».

Автори дослідження [8] провели комплексний аналіз за допомогою тестування на проникнення в систему зарядного пристрою і пов'язані з ним системи для оцінки вразливості безпеки. За допомогою різних методів, таких як перехоплення мережевого трафіку, імітація атак і спуфінг, було виявлено кілька потенційних недоліків безпеки, якими можуть скористатися зловмисники. Тому застосування стандарту ISO 15118-20 дозволяє зберігати та передавати дані користувачів без ризику їхнього витоку у компонентах зарядної інфраструктури.

Такі вимоги безпеки є обов'язковими для комунікації електромобіля та зарядного пристрою, коли автомобіль ідентифікує себе й авторизує передачу електроенергії. Це пов'язано з тим, що зарядний пристрій передає повідомлення між електромобілем і постачальником послуг зарядної станції. Втім, безпека даних може перебувати на низькому рівні, коли використовуються альтернативні засоби авторизації, такі як радіочастотна ідентифікація (RFID) і комунікації близького радіусу дії смартфона (NFC), що пов'язують власника електромобіля із зарядною станцією. При цьому корпуси зарядних пристроїв не забезпечують належного фізичного захисту від несанкціонованого доступу.

Як показує досвід, зловмисники все частіше використовують програмне забезпечення, щоб отримати доступ до смартфона (наприклад, вдалий обхід захисту операційної системи IOS), а в електромобілі, щоб обійти електронний замок на дверях і систему

дистанційного запуску (як приклад, Hyundai і KIA випуску 2022 року).

Маніпуляції з бортовими електронними блоками управління електромобіля, що здійснюються, зокрема, за допомогою смартфону, дають можливість втручатися в системи керування і гальмування, управління двигуном і акумулятором. На будь-якому етапі передачі сигнали можуть дистанційно перехоплюватись, що дає фізичний доступ до електромобіля або конфіденційної інформації власника.

Навіть за умови застосування нових стандартів кібербезпеки зв'язку вразливими точками доступу до електромобіля залишаються бездротовий зв'язок для обміну інформацією з додатками для смартфонів, порт USB та система OBD [9].

Завдяки широкому спектру кіберсистем електромобіля з'являється можливість проникнути в мережу зарядних станцій, оскільки оператор зарядної станції пов'язаний з оператором розподільчої мережі через протокол Open Smart Charging Protocol (OSCP). Цей протокол забезпечує інтерактивний обмін даними між операторами з метою оптимального узгодження споживання електроенергії. Оператор послуг має доступ до інших зарядних пристроїв міста через зв'язок OSCP, що дає можливість зловмиснику отримати доступ до інфраструктури та вплинути навіть на енергетичну безпеку міста [10].

У майбутньому виробники електромобілів та оператори зарядних станцій мають визначитися, чи зможуть електромобілі заряджатися, використовуючи вразливі протоколи зв'язку згідно зі стандартом ISO 15118-2, для раніше випущених електро-мобілів, якщо автомобіль або зарядна станція не відповідають вимогам ISO 15118-20.

Отже, на цей час протоколи для зв'язку в галузі заряджання електромобілів не стандартизовані, але тривають спроби розробити відповідний стандарт.

Висновки

Основними точками доступу хакерів до електронних систем електромобіля є бездротовий зв'язок для обміну інформацією, порт USB та система бортової діагностики, а короткі ключі шифрування даних та занадто тривалі терміни їхньої дії сприяють несанкціонованому доступу до системи.

Зі свого боку виробники електромобілів та оператори зарядних станцій мають визначитися, чи зможуть раніше випущені електромобілі заряджатися, використовуючи небезпечні протоколи зв'язку згідно зі старим стандартом, якщо автомобіль або зарядна станція не відповідають вимогам стандарту ISO 15118-20, який передбачає використання алгоритмів цифрового підпису.

Також швидкому впровадженню технології «plug-and-charge» за стандартом ISO 15118-20 заважає відсутність консенсусу серед виробників автомобільної галузі і відсутність стандартизації зарядних пристроїв і комунікаційних протоколів. Тому є нагальна потреба зробити стандарт ISO 15118-20 частиною програми субсидій для громадської звичайної та швидкої зарядної інфраструктури.

References

1.UN. (2021). UN Regulation No. 155 – Cyber security and cyber security management system. Retrieved from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

2.Alessandro Brighente, Mauro Conti, Denis Donadel, Radha Poovendran, Federico Turrin, & Jianying Zhou (2023). Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. Retrieved from: https://readpaper.com/paper/4711095084272074753

3.ENCS. (2019). Security requirements for procuring EV charging stations. Retrieved from: https://encs.eu/resource/ev-301-2019-security-requirements-for-procuring-ev-charging-stations/springeropen.com/articles/10.1186/s42162-022-00190-y#citeas

4.Zhang, H.; Meng, X.; Zhang, X.; Liu, Z. (2020). CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. *Sensors* 2020, *20*, 4900. Retrieved from: https://www.mdpi.com/ 1424-8220/20/17/4900

5.ISO. (2022). ISO 15118-20:2022(en) Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements. Retrieved from: https://www.iso. org/obp/ui/ru/#iso:std:iso:15118:-20:ed-1:v1:en

6.Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis and C. Douligeris, (2022)."Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)," in IEEE Communications Surveys & Tutorials, vol. 24, 3, 1504-1533, thirdquarter. Retrieved from: https://ieeexplore.ieee.org/document/9800931

7.DfT. (2021). Electric vehicle smart charging consultation: summary of responses. Retrieved from: https://www.gov.uk/government/consultations/electric-vehicle-smart-charging/public-feedback/electric-vehicle-smart-charging-consultation-summary-of-responses

8.Johnson, J.; Berg, T.; Anderson, B.; Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* 2022, *15*, 3931. Retrieved from: https://www.mdpi.com/1996-1073/15/11/3931

9.Unterweger, A., Knirsch, F., Engel, D. *et al.* (2022).An analysis of privacy preservation in electric vehicle charging. *Energy Inform* 5, 3.

10.Acharya, S., Dvorkin, Y., Pandžić, H. and Karri, R. (2020). "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," in IEEE Access, vol. 8, 214434-214453. Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9272723&isnumber=8948