Кибератаки на зарядные станции

Д.Е. Намиот, А.А. Пичугов, А.П. Мякишев

***Аннотация*—Доля электротранспорта во всех странах неуклонно растет. Зарядная инфраструктура, очевидно, является одним из определяющих моментов для этого роста. Эта инфраструктура (ее работоспособность) является критическим элементом для электроавтомобилей. И именно эта инфраструктура становится целью кибератак. Основная проблема безопасности заключается в том, что, когда электромобиль подключается к зарядной станции, автомобиль и зарядная станция взаимодействуют друг с другом с помощью сетевого соединения. Это соединение осуществляется по линии электропередачи зарядного кабеля. И модем, отвечающий за это взаимодействие, доступен как обычный сетевой интерфейс на контроллере зарядной станции. Из-за этого неправильная настройка служб на контроллере зарядной станции (их компрометация) может привести к тому, что эти службы будут доступны на зарядном кабеле, что открывает большие возможности для кибератак. Стремление обеспечить удобство и гибкость процесса зарядки, в определенной степени, вступает в противоречие с необходимостью обеспечения безопасности. Все это привело к тому, что появляется все больше примеров проблем кибербезопасности именно для зарядных станций и связанной с ними инфраструктуры, которая также может быть атакована.**

***Ключевые слова*—электротранспорт, зарядки, кибератаки.**

I. Введение

Зарядная инфраструктура для электромобилей является одним из ключевых элементов развития рынка электромобилей. Существует стратегия развития зарядной инфраструктуры России, которая предусматривает создание сети зарядных станций по всей стране. Наличие инфраструктуры, очевидно, будет играть ключевую роль в переходе на экологически чистый вид транспорта.

“Развитие сети зарядок в столице – важная часть утвержденной стратегии развития транспортной системы Москвы и области на период до 2035 г.

К 2035 г. в Москве и области доля электрического транспорта составит 15%. Это около 1 млн. автотранспортных средств” [1].

Глобально, в мире сейчас приходится порядка 10 электро-автомобилей на одну публичную зарядку. При этом распределение по странам очень неравномерное. В 2023 году из 4 миллионов установленных станций, 70% приходилось на один Китай [2]. Международное энергетическое агентство (IEA) называет цифру в 15 млн. станций к 2030 году.

Во множестве исследовательских и прогнозных работ отмечается, что именно доступность инфраструктуры будет являться определяющим моментом для развития электротранспорта. Например, в работах [3, 4] отмечается, что одной из главных проблем расширения внедрения электромобилей являются сомнения водителей, которые проявляется через понятие “анксетия дальности” (*range anxiety*) – боязнь водителей остаться без заряда в пути, что становится одной из главных причин отказа от покупки электромобиля. Путь для снижения этой тревожности только один – необходима достаточная плотность зарядных станций с достаточной мощностью для быстрого заряда батареи, и их правильное пространственное распределение. Именно плотная и мощная сеть электрозарядок (электрозаправок) разного типа (быстрых, медленных, переменным и постоянным током) является главным условием для повышения доверия к электромобилям как к надежному средству передвижения.

Очевидно, что такие сети, обеспечивающие движение электротранспорта, будут относиться к критической инфраструктуре. Критическая информационная инфраструктура (КИИ) – это совокупность информационных систем и телекоммуникационных сетей, критически важных для работы ключевых сфер жизнедеятельности государства и общества: здравоохранения, промышленности, связи, транспорта, энергетики, финансового сектора и городского хозяйства [5].

Есть множество работ, которые посвящены именно планированию размещения зарядных станций [6, 7]. Но очевидно, что размещенные станции должны работать, и здесь появляются проблемы, связанные с кибератаками на такого рода системы. Опубликованных примеров таких атак уже довольно много. Например, атаки с удаленным выключением зарядных станций и размещением собственной информации на мониторах зарядных станций [8], атаки на зарядные станции в Великобритании [9] и т.д. На конференции Hardwear.io отмечалось, что, в то время как многие производители, по-видимому, сосредоточены на качестве электроэнергии и совместимости, защита зарядных станций от вредоносных сообщений, по-видимому, была второстепенной, если вообще когда-либо рассматривалась. В представленной на конференции презентации авторы протестировали устройства от 13 производителей, включая 18 зарядных станций постоянного тока и одну зарядную станцию переменного тока, обнаружив недостатки в половине

Статья получена 9 января 2025.
Д.Е. Намиот – МГУ имени М.В. Ломоносова, ORCID: https://orcid.org/0000-0002-4463-1678 (dnamiot@gmail.com)
А.А. Пичугов – МГУ имени М.В. Ломоносова, ORCID: https://orcid.org/0009-0001-3489-7915 (pichugov.a.a@cs.msu.ru)
А.П. Мякишев – НТЦ "Вулкан"; МГУ имени М.В. Ломоносова, ORCID: https://orcid.org/0009-0003-7448-3930 (a.myakishev@ntc-vulkan.ru)

продуктов. Например, из зарядных устройств восемь оставили SSH порт открытым, два открыли HTTP, и одно открыло сетевой протокол MQTT между машинами, в то время как другие открыли различные фирменные сервисы [10].

Основная проблема безопасности заключается в том, что когда электромобиль подключается к зарядной станции, автомобиль и зарядная станция взаимодействуют друг с другом. То есть, при подключении вашего электромобиля к станции быстрой зарядки постоянного тока автомобиль будет взаимодействовать с зарядной станцией с помощью сетевого соединения. Это соединение осуществляется по линии электропередачи зарядного кабеля. И модем, отвечающий за это взаимодействие, доступен в Linux как обычный сетевой интерфейс. Из-за этого неправильная настройка служб на контроллере зарядной станции может привести к тому, что эти службы будут раскрыты (доступны) на зарядном кабеле.

Все это привело к тому, что появляется все больше работ, описывающих проблемы кибербезопасности именно для зарядных станций и связанной с ними инфраструктуры, которая также может быть атакована [11, 12]. Обзор проблем кибербезопасности зарядных станций и связанной с ними инфраструктурой и есть тема настоящей статьи.

Статья подготовлена в рамках реализации совместной образовательной программы ПАО Сбербанк – магистратуры “Кибербезопасность” на факультете вычислительной математики и кибернетики МГУ имени М. В. Ломоносова [13-15].

Оставшаяся часть статьи структурирована следующим образом. В разделе II рассматривается системная архитектура и существующие стандарты для системы зарядок электротранспорта. В разделе III – поверхность атак для киберфизических систем. Раздел IV посвящен собственно атакам на системы зарядок. И в разделе V обсуждается защита.

II. Системная архитектура и стандарты

Экосистема зарядки электромобилей представляет собой динамическую киберфизическую систему (CPS), которая включает в себя взаимосвязанные аппаратные и программные элементы [16]. Темой обзора, естественным образом, является программная часть этой экосистемы.

Экосистема зарядки состоит из трех основных компонентов: EV (электромобили), EVCS (зарядные станции) и Централизованная система управления (CMS) [17]. Электромобиль полагается на эти системы для эффективного управления процессом зарядки.

EVCS состоит из одного или нескольких блоков оборудования для питания электромобилей и подает питание на электромобили.

CMS - облачная компонента, основная роль которой заключается в мониторинге и управлении различными зарядными станциями. CMS осуществляет планирование и контроль процесса зарядки, ведение журналов, управление транзакциями, а также проведение удаленной диагностики и корректировки [18]. Естественно, эти компоненты должны опираться на надежные каналы связи для обеспечения эффективного управления энергопотреблением, безопасных платежных транзакций и эффективной координации.

Обмен данными осуществляется между системой управления аккумуляторными батареями электромобилей и EVCS, между EVCS и CMS, а также между CMS, поставщиками энергии и электросетью [12]. На рисунке 1 приведено схематическое изображение этой структуры.

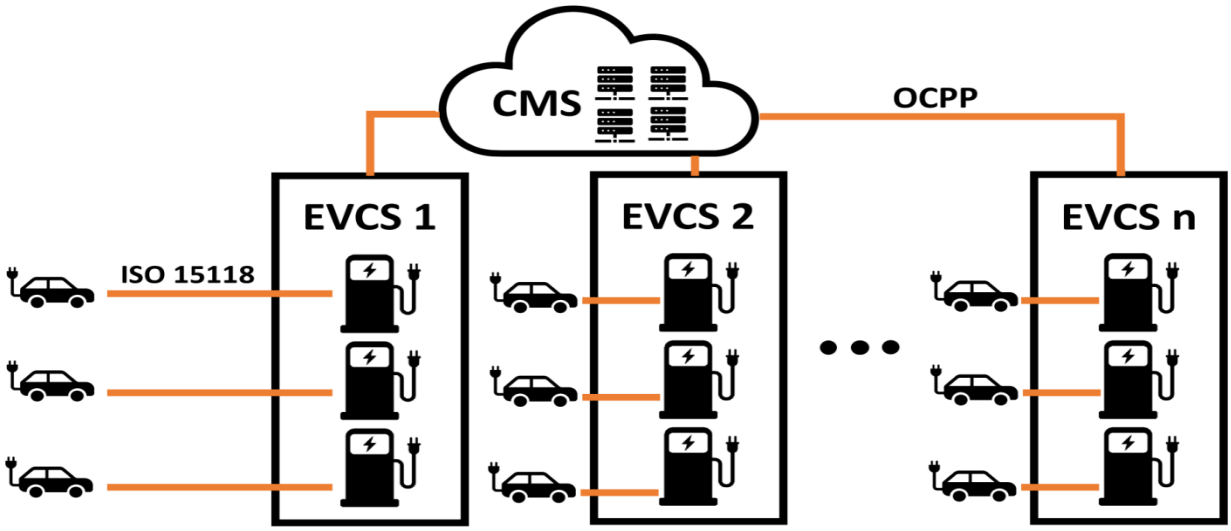

Рис. 1. Схема связи между EV и EVCS (ISO 15118) и между EVCS и CMS (OCPP) [17]

Во всем мире для EVCI используются различные стандарты. ISO 15118, OCPP, SAE, CHAdeMO и IEC являются одними из самых известных стандартов в области зарядки электромобилей [19].

ИСО 15118 – это протокол Международной организации по стандартизации (ISO) 15118, который был специально разработан для связи между электромобилями и EVCS [16]. Протокол позволяет согласовывать надлежащий график зарядки, а также обеспечивать защиту от несанкционированного доступа или вмешательства. Стандарт ISO 15118 обеспечивает безопасную связь между электромобилями и EVCS, предотвращая перехват и изменение сообщений злоумышленниками или фальсификацию платежной информации. Это достигается за счет внедрения функции *Plug&Charge* [20], что требует установления защищенного канала связи между электромобилем и EVCS. Эта функция использует цифровые сертификаты для безопасной связи и обеспечивает автоматическую аутентификацию и авторизацию [20]. Протокол также определяет структуры и форматы сообщений, которыми обмениваются электромобили и EVCS. В нем указано, как электромобили и EVCS должны шифровать и расшифровывать сообщения, что обеспечивает конфиденциальность и целостность связи [21]. Стандарт ISO 15118 устанавливает требования как к физическому, так и к канальному уровню [20].

Open Charge Point Protocol (OCPP) – это открытый и широко распространенный протокол связи для зарядных станций для электромобилей [21]. OCPP упрощает обмен данными между EVCS и CMS. Основные функции протокола OCPP связаны с управлением процессами зарядки и бронирования с учетом ограничений безопасности. Его основная цель заключается в том, чтобы гарантировать, что списание средств происходит только после авторизации платежной системой, тем самым устраняя потенциальные мошеннические действия, связанные с платежными системами. Протокол включает в себя такие функции, как безопасное обновление встроенного ПО, ведение журнала безопасности, уведомление о событиях и аутентификация. OCPP использует TLS для обеспечения безопасной связи и реализует управление ключами для сертификатов на стороне клиента [21]. К другим ключевым особенностям OCPP относятся поддержка стандартов электросетей, возможности дистанционного управления и интеллектуальные сценарии зарядки с помощью профилей зарядки. С помощью OCPP, CMS может удаленно запускать/останавливать процессы зарядки, контролировать и изменять состояние зарядной станции, а также внедрять интеллектуальные профили зарядки, указывая пределы мощности и продолжительность для оптимального управления зарядкой в течение дня.

Стандарты Общества автомобильных инженеров (SAE) охватывают как физические, так и коммуникационные протоколы между электромобилем и EVCS. Стандарт SAEJ2293 учитывает требования к электропитанию, архитектуре системы и коммуникационным требованиям для зарядки электромобилей. SAEJ1772 определяет номинальные характеристики оборудования для зарядки переменным током (AC) и постоянным током (DC) с различными доступными уровнями зарядки. SAEJ1773 фокусируется на схемах зарядки с индуктивной связью, включая требования к ручному подключению и программному интерфейсу. SAEJ2847 определяет требования к связи и сценарии использования между электромобилями и зарядной инфраструктурой, устанавливая требования к цифровой связи между интерфейсами электромобилей, EVSE, коммунальных служб и энергетических услуг. SAEJ2954 содержит спецификации для беспроводной зарядки и включает такие функции, как помощь при вождении и автономная зарядка.

Стандарт CHAdeMO охватывает как физические, так и коммуникационные аспекты. Что касается физического аспекта, CHAdeMO определяет физический разъем и характеристики зарядки для быстрой зарядки высоковольтным постоянным током. Протокол CHAdeMO используется для связи между EVCS и EV, обеспечивая оптимальную и быструю зарядку на основе команд EV. Зарядные устройства CHAdeMO популярны в Японии и Европе. CHAdeMO, хотя и поддерживает операции Vehicle-to-Grid (V2G), имеет определенные ограничения. С точки зрения связи, одним из основных недостатков является отсутствие функций безопасной связи, вместо этого они полагаются на связь по сети контроллеров (CAN). CAN позволяет электронным компонентам в автомобиле взаимодействовать друг с другом, не полагаясь на центральный компьютер. Это подвергает CAN-шину автомобиля потенциальным рискам безопасности, поскольку незашифрованная связь делает ее уязвимой для контроля или программирования со стороны злоумышленников [17].

Стандарты Международной электротехнической комиссии (МЭК/IEC), такие как IEC 61851, IEC 61980 и IEC 62196, охватывают физические и нефизические аспекты систем зарядки электромобилей. Эти стандарты регулируют протоколы и интерфейсы, используемые для связи между электромобилями и EVCS. Они охватывают общую эксплуатацию, бортовое и внешнее оборудование, а также конкретные компоненты, используемые в зарядке электромобилей. Например, IEC 61851 устанавливает стандарт для кондуктивных зарядных систем, IEC 61980 относится к системам беспроводной передачи мощности (WPT), а IEC 62196 определяет спецификации для вилок, разъемов и входов, используемых в кондуктивной зарядке (наиболее широко используемый метод зарядки электромобиля, который распределяет мощность от электросети к электромобилю по проводу). Эти стандарты обеспечивают безопасность, совместимость и надежность физических компонентов, участвующих в зарядке электромобилей, предоставляя рекомендации для производителей, установщиков и пользователей Недостатком стандарта IEC является то, что он не предоставляет конкретных стандартов для обратного потока мощности в электромобилях – обратный поток мощности относится к способности электромобилей подавать энергию обратно в сеть [17].

Использование стандартизированных протоколов снижает уязвимости, вызванные разнообразным набором протоколов, и упрощает управление системой, сводя к минимуму риск эксплуатации и ошибок при

интеграции.

Модельная системная архитектура представлена на рис.2. В работе [22] была уточнена ее структура, EVCS выступает как шлюз к нескольким зарядкам, и вся конфигурация состоит из нескольких ключевых компонентов, а именно: интеллектуального EVSE, брокера MQTT, CMS и мобильного приложения (рис 3).

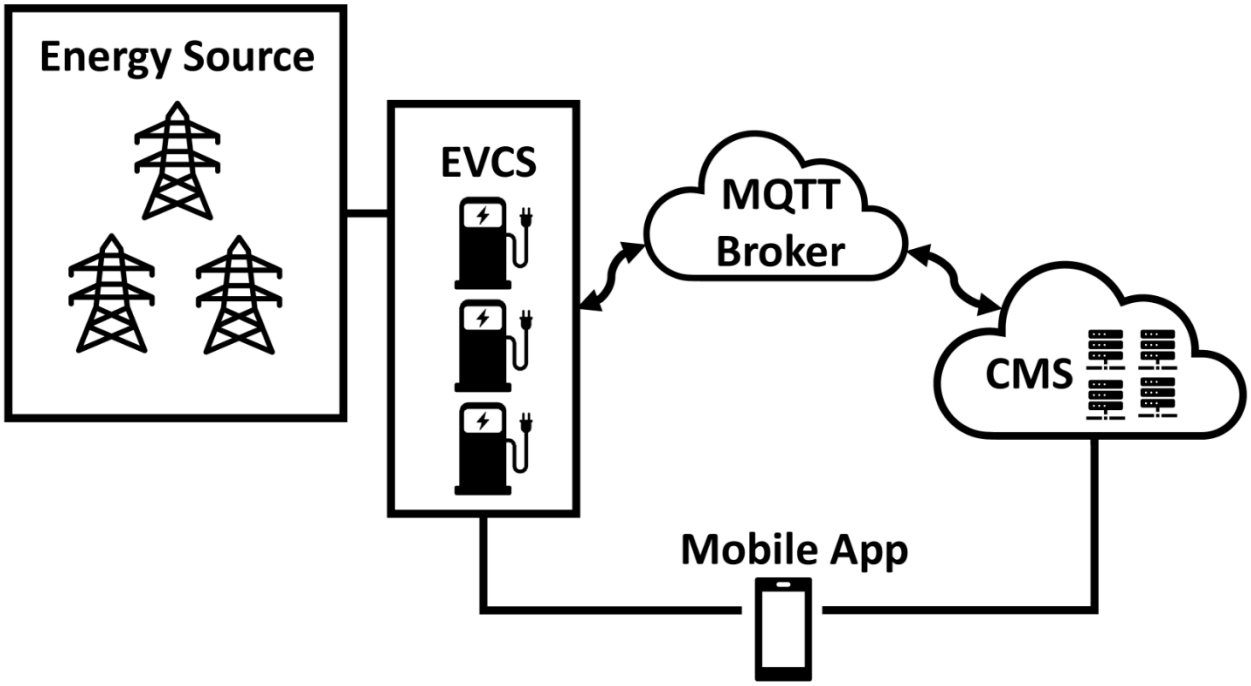

Рис. 2. Системная архитектура [17]

Интеллектуальное устройство EVSE предназначено для интеллектуальной зарядки электромобилей, мониторинга зарядной активности и связи с CMS по протоколу MQTT. Устройство использует уникальный QR-код для идентификации, контролирует процесс зарядки и обеспечивает наличие механизмов безопасности. Микроконтроллер ESP8266 используется для координации зарядки и связи, а модуль Wi-Fi обеспечивает подключение к Интернету. Брокер MQTT выступает в качестве коммуникационного узла, облегчая обмен информацией о состоянии между интеллектуальными устройствами EVSE и CMS. CMS отвечает за управление и координацию зарядных операций, учет использования энергии и предоставление дополнительных услуг. Мобильное приложение позволяет пользователям удаленно запускать и останавливать сеансы зарядки, отслеживать статистику использования и получать доступ к актуальной информации. Эта интегрированная архитектура обеспечивает бесконтактную и эффективную зарядку для владельцев электромобилей [22]. На рисунке 3 показана общая структура и задействованные компоненты.

В этой интеллектуальной системе зарядки между компонентами происходит обмен различными сообщениями для обеспечения бесперебойной зарядки. Интеллектуальное устройство EVSE обменивается данными с центральным веб-сервером управления по протоколу MQTT. Основные сообщения, которыми обмениваются смарт-EVSE и сервер, включают сообщение *Boot_Notification*, которое отправляется устройством при включении питания для уведомления сервера о его присутствии и готовности. Сообщение *Device_Healthy* непрерывно публикуется интеллектуальным EVSE для указания его рабочего состояния. Сообщение *Device_Start* используется для инициирования сеанса зарядки, в то время как сообщение *Device_StopCharging* отправляется для сигнализации о завершении процесса зарядки. Эти сообщения позволяют регистрировать устройство, отслеживать состояние и контролировать процесс зарядки.

CMS обменивается данными с интеллектуальным EVSE через брокер MQTT, а сообщения *Remote_start* и *Remote_stop* используются для удаленного управления сеансами зарядки, позволяя серверу начать или остановить зарядку на устройстве. Кроме того, мобильное приложение используется для инициирования и мониторинга сеансов зарядки. Мобильное приложение также предоставляет доступ к статистике использования и позволяет осуществлять бесконтактную зарядку [17, 22]. Мобильное приложение взаимодействует с сервером управления, который затем взаимодействует со смарт-EVSE с помощью брокера MQTT.

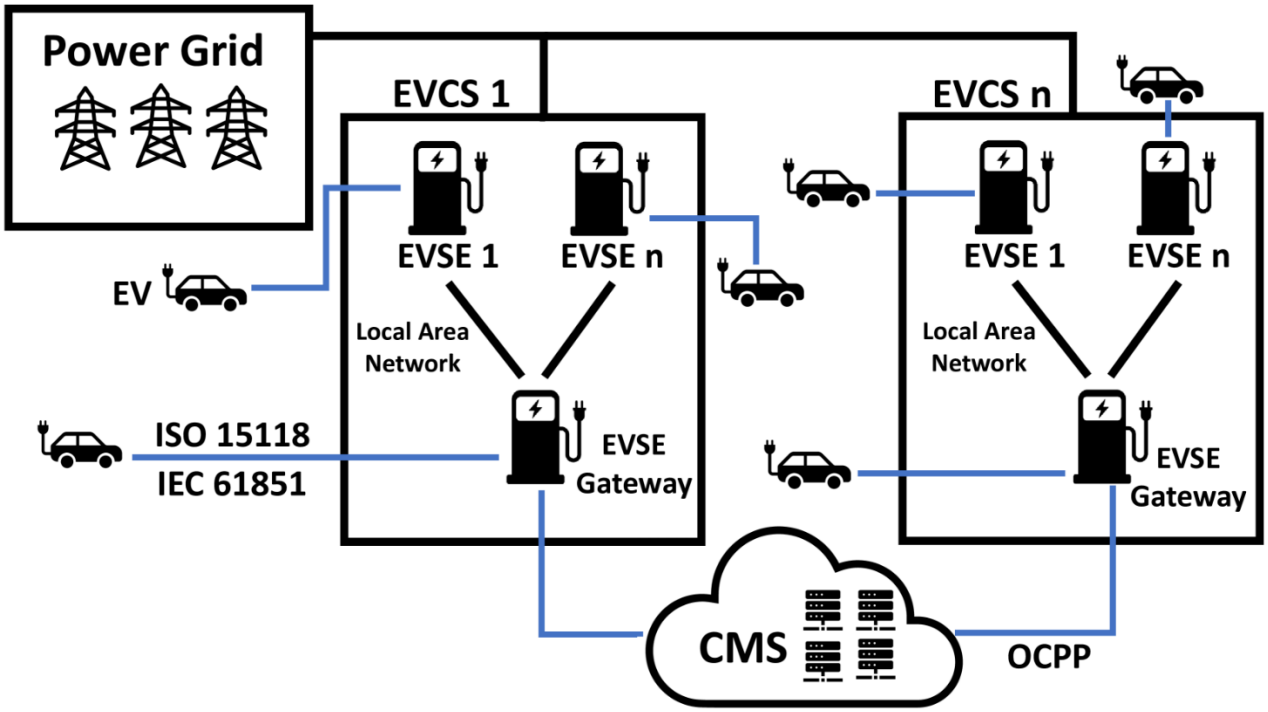

Рис. 3. Компоненты инфраструктуры (EVCI) [17]

Связь между мобильными приложениями и CMS происходит по протоколу HTTPS, включая SSL/TLS для безопасной и зашифрованной связи. Мобильные приложения предлагают такие функции, как обнаружение ближайшей EVCS, удаленный запуск/остановка сеансов зарядки и планирование зарядки, обеспечивают удаленный мониторинг и управление EVCS.

Кроме того, CMS предоставляет конечные точки API для связи между мобильным приложением и EVCS. У каждого оператора есть (может быть) своя CMS, отвечающая за такие задачи, как бронирование, планирование, платежи и мониторинг. CMS взаимодействует с EVCS с помощью OCPP. На рисунке 5 представлен обзор взаимодействий в экосистеме зарядки электромобилей.

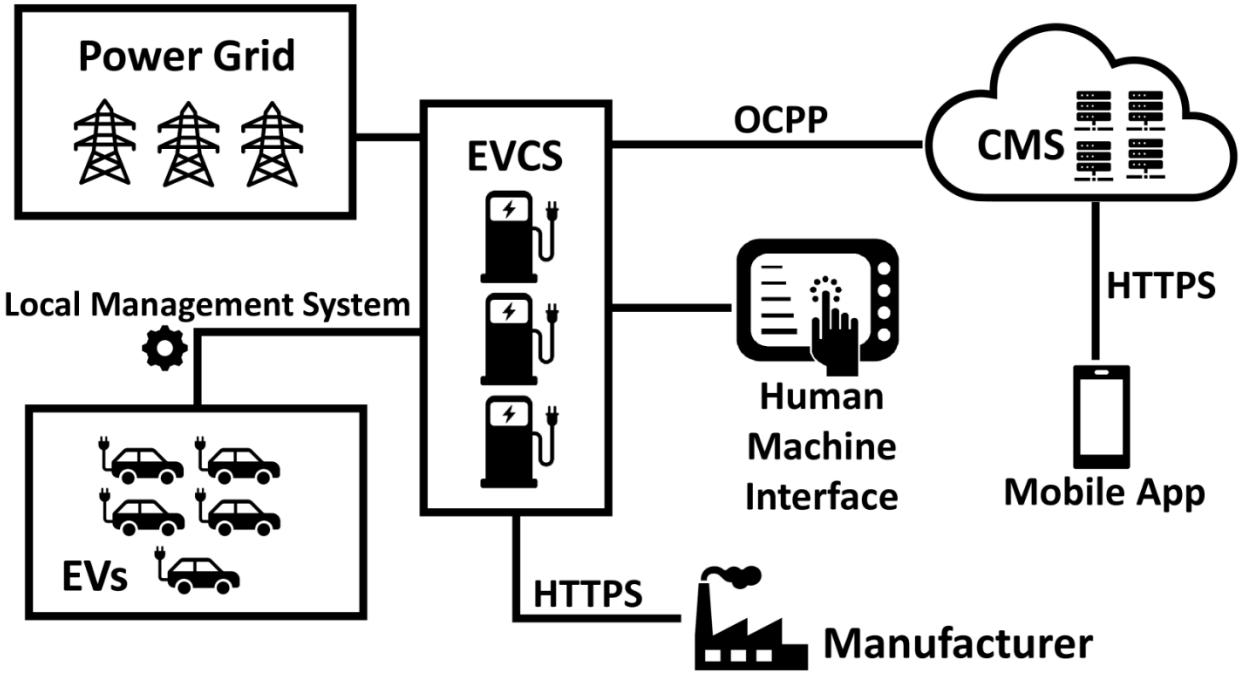

Рис. 4. Обзор взаимодействия [17]

III. Атаки на киберфизические системы

Популярный учебник в области кибербезопасности CyBOK [23] приводит классическую схему классификации атак на киберфизические системы (рис. 5).

Цифрами обозначены различные атаки. В качестве контроллера в случае инфраструктуры зарядок выступает CMS.

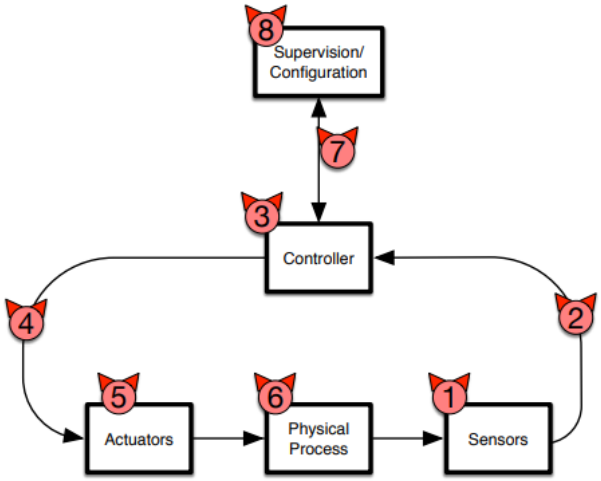

Рис. 5. Поверхность атак для CPS [23]

1. Атака 1 представляет собой злоумышленника, который скомпрометировал датчик (например, если данные датчика не аутентифицированы или если у злоумышленника есть ключевой материал для датчиков) и вводит ложные сигналы датчика, заставляя управляющую логику системы действовать на основе вредоносных данных.
2. Атака 2 представляет собой злоумышленника на пути связи между датчиком и контроллером, который может задержать или даже полностью заблокировать информацию от датчиков контроллеру, поэтому контроллер теряет наблюдаемость системы (потеря обзора), тем самым заставляя ее работать с устаревшими данными. Примерами таких атак являются атаки типа “отказ в обслуживании” на датчики и атаки на устаревшие данные.
3. Атака 3 представляет собой злоумышленника, который скомпрометировал контроллер и отправляет неправильные управляющие сигналы исполнительным механизмам.
4. Атака 4 представляет собой злоумышленника, который может задержать или заблокировать любую команду управления, тем самым вызывая отказ в управлении системой. Эта атака может быть рассмотрена как отказ в обслуживании исполнительных механизмов.
5. Атака 5 представляет собой злоумышленника, который может скомпрометировать исполнительные механизмы и выполнить управляющее действие, которое отличается от того, что намеревался сделать контроллер.
6. Атака 6 представляет собой злоумышленника, который может физически атаковать систему (например, физически уничтожить часть инфраструктуры и объединить это с кибератакой). Это тип совместной кибер- и физической атаки.
7. Атака 7 представляет собой злоумышленника, который может задерживать или блокировать связь с системой контроля и управления или устройствами конфигурации.
8. Атака 8 представляет собой злоумышленника, который может скомпрометировать или выдать себя за систему SCADA (регистрации данных) или устройства конфигурации и отправить вредоносные изменения управления или конфигурации.

Приводимые ниже атаки являются иллюстрацией этой классификации.

IV. Сценарии Атак на инфраструктуру зарядки (ECVI)

Кибератаки на EVCI могут проявляться в различных формах. Поскольку система связи служит основой EVCI, выполняя такие важные операции, как планирование электромобилей, аутентификация и интеграция в сеть, любая компрометация в этой коммуникации может сделать всю EVCI уязвимой [24]. У злоумышленников существуют разные мотивы, начиная от кражи электроэнергии и заканчивая нарушением работы сети зарядных станций [25].

Взаимосвязанный характер электромобилей и зарядных станций создает серьезные проблемы с точки зрения безопасности и надежности. EVCI подвержены широкому спектру угроз кибербезопасности, таким как DoS-атаки, атаки MitM (*Man in the middle*), подслушивание, спуфинг, внедрение ложных данных (FDI), взлом, программы-вымогатели, троянские вирусы, внедрение вредоносного ПО и утечки данных. Эти угрозы могут привести к утечке личных или финансовых данных и захвату энергетической или зарядной инфраструктуры [26].

Постоянная связь между EVSE и интеллектуальными сетями означает, что слабые места в зарядных станциях могут иметь далеко идущие последствия для всей сети. Критически важный обмен информацией происходит во время зарядки автомобиля или когда пользователи взаимодействуют со своими автомобилями через программное обеспечение, создавая потенциальное узкое место, где конфиденциальные данные и конфиденциальность пользователей могут быть поставлены под угрозу. Обеспечение безопасности этой взаимосвязанной инфраструктуры имеет решающее значение для сохранения конфиденциальности пользователей и обеспечения надежной работы сети [27]. В этой работе приводится список профилей безопасности для электроавтомобилей (рис. 6).

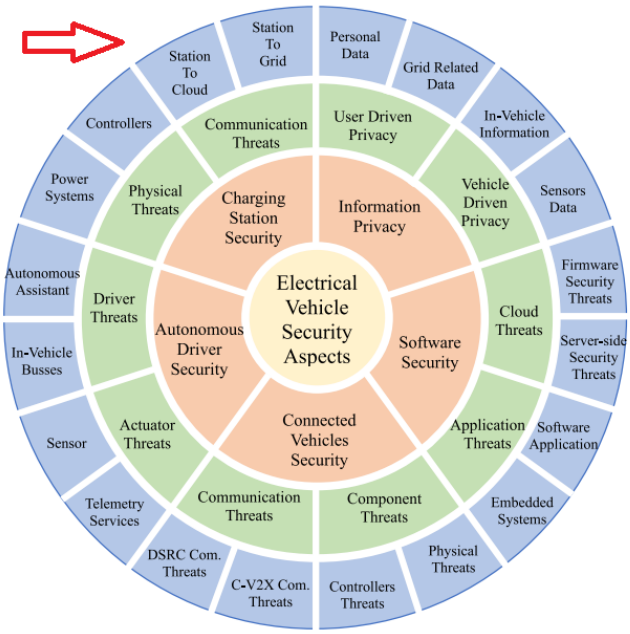

Рис. 6. Профили безопасности электромобиля

Проблемы безопасности зарядной инфраструктуры разделены здесь на физические и коммуникационные. В качестве последних рассматриваются атаки на взаимодействие зарядной станции с облаком (CMS) и электросетевой инфраструктурой (GRID). Здесь же приводится большой список известных атак (рис.7). Атаки разделены на следующие группы:

- Спуфинг: например, подмена устройства зарядки или CMS при обмене, подбор паролей для аутентификации в системе, перехват и анализ данных при обмене между электромобилем и зарядной станцией;
- Подделка (например, подделка данных зарядной сессии);
- Трекинг данных: модификация данных зарядных сессий и передач OCPP;
- Раскрытие информации: кража данных зарядных сессий, атаки по побочным каналам;
- Отказ в обслуживании: атаки отказа в обслуживании для зарядных станций и облачных сервисов;
- Подъем привилегий: привилегированный доступ к зарядным станциям и облачным сервисам.

На что здесь можно обратить внимание? Быстрые зарядки с высокой мощностью (значительным потоком энергии) сами по себе представляют физическую опасность. Атаки на зарядные станции могут привести к потере доступности зарядки электромобилей или проблемам с безопасностью из-за перезарядки аккумулятора. Кроме того, злоумышленники могут манипулировать скоростью зарядки, блокировать сеансы зарядки или даже разряжать аккумуляторы, что представляет значительный риск, как для владельцев электромобилей, так и для операторов зарядных станций.

Одной из опасных (и относительно легко реализуемым) методов атак является атака отказа в обслуживании (DoS), когда злоумышленник перегружает CMS или EVSE чрезмерным трафиком или

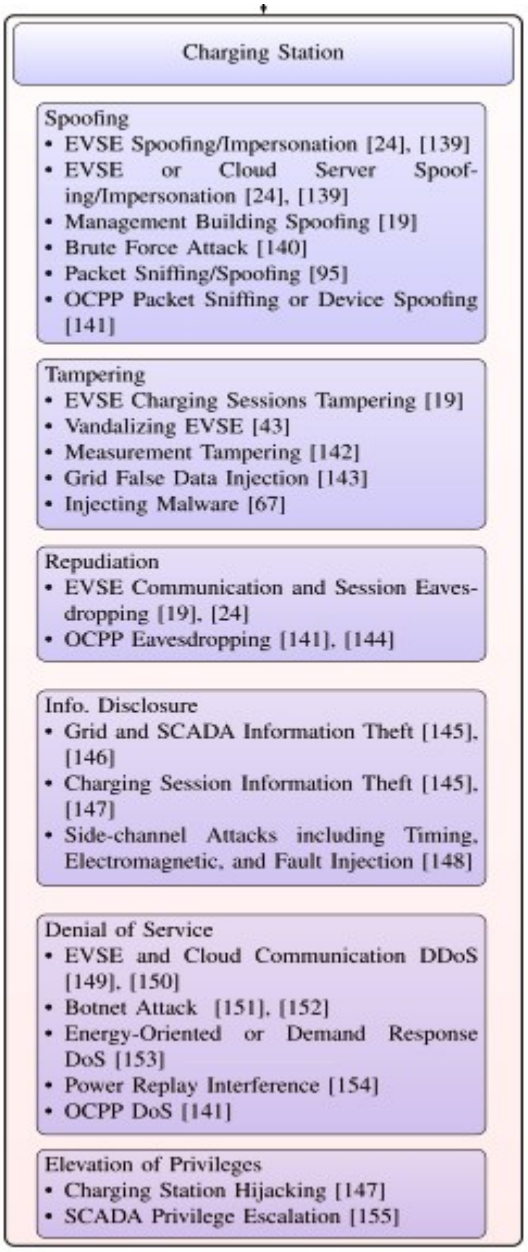

Рис. 7. Атаки на инфраструктуру зарядки [27]. Ссылки – по библиографическому списку обзора [27].

высокими запросами на зарядку, что приводит к сбою системных ресурсов или их зависанию. DoS-атаки могут быть инициированы различными способами, например, с помощью ботнетов или флуда. В исследовании [28] использовали поддельные IP-адреса законных EVSE для запуска DoS-атак. Еще одна потенциальная форма DoS-атаки включает в себя переполнение CAN-шины электромобиля большими объемами трафика или поддельными сообщениями, что может насытить шину и нарушить способность транспортного средства выполнять нормальные операции, тем самым препятствуя обработке транспортным средством законных управляющих сообщений. Кроме того, если канал связи между электромобилем и зарядными станциями перегружен чрезмерным количеством запросов на подключение или неправильно сформированными пакетами, коммуникационные возможности автомобиля могут быть серьезно нарушены. Иными словами (и это также следует из

рис. 6), атака на зарядную станции может идти со стороны электромобиля.

В работе [25] отмечается, что DoS-атака на EVCS часто начинается с атаки спуфинга, когда злоумышленник компрометирует уникальный идентификатор устройства, такой как MAC-адрес, что позволяет ему маскироваться под законного пользователя. Как только злоумышленник получает несанкционированный доступ к системе, он нацелен на CMS или EVSE, наводняя сеть чрезмерным трафиком или запросами на высокую тарификацию. Варианты атак, такие как UDP или TCP/IP-флуд, низкоскоростные DoS-атаки, пинг-флуд или ICMP-payload, могут вывести из строя зарядную станцию или другие узлы в сети зарядной станции. Эта атака перегружает системные ресурсы, вызывая сбой CMS или переставая отвечать, фактически препятствуя доступу законных пользователей к услугам тарификации. Чтобы смягчить такие атаки, операторы EVCS должны внедрить надежные механизмы аутентификации, фильтрацию трафика, ограничение скорости и методы обнаружения аномалий для выявления и предотвращения аномальных моделей трафика.

Еще одной серьезной угрозой является манипуляция прошивкой, когда злоумышленники модифицируют прошивку зарядной станции, внедряя вредоносный код, потенциально влияющий на процессы, управляющие действия и условия работы системы. Этот вредоносный код может принимать форму вирусов, программ-вымогателей или атак с использованием SQL- и XSS-инъекций [25]. Кроме того, злоумышленники могут использовать разъемы EV для установки вредоносного ПО или манипулирования настройками зарядки, обеспечивая несанкционированный доступ к EVCS [26].

Отсутствие надежной защиты в программных модулях делает зарядные станции и облако уязвимыми для вредоносного ПО, что позволяет проводить скоординированные атаки, которые могут отключить всю сеть или повлиять на электросеть путем одновременной активации нескольких зарядных станций [25].

Более сложная атака, известная как Malicious Mode Attack (MMA) [29] состоит в скоординированной отправки команд принудительного управления колебаниями на несколько зарядных станций. Эта атака приводит к высокоамплитудным вынужденным колебаниям в энергосистеме, что приводит к нестабильности системы и нарушению энергоемкости АСУ ТП [30].

OCPP, один из наиболее широко используемых протоколов на зарядных станциях, не имеет встроенных мер безопасности от кибератак, что потенциально предоставляет неавторизованным пользователям точку доступа и оставляет уязвимости для атак MitM. Злоумышленник может использовать функцию минимальной длительности состояния в OCPP для доступа к интерфейсу связи между EVCS и CMS. Оказавшись внутри, злоумышленник манипулирует электромобилями и точками зарядки, изменяя основные функции запуска или остановки транзакций, чтобы перезарядить батареи или полностью предотвратить их зарядку, что потенциально создает опасные ситуации или создает неудобства для потребителей, которым потребуется зарядка позже [31].

Атаки MitM часто используются в радиосвязи между EVSE, подключаемыми электромобилями (PEV) и системами управления энергопотреблением зданий (BEMS). Злоумышленник может повредить данные или получить полный контроль над узлом, передав неверную информацию, такую как ложное состояние зарядной станции [25]. Кроме того, атаки MitM могут происходить во время процесса аутентификации и авторизации между PEV и зарядными станциями или на протяжении всей зарядной сессии. Несмотря на соответствие стандарту безопасности ISO 15118, канал связи по-прежнему подвержен атакам MitM. В этих атаках злоумышленник перехватывает и манипулирует данными, которыми обмениваются зарядная станция и транспортное средство. Маскируясь под законного участника, злоумышленник может получить несанкционированный доступ, что может привести к краже транспортных средств, информации или энергии [27].

В сценарии атаки, предложенном в работе [18], злоумышленник может манипулировать EVCS, чтобы создать узкое место на дорогах, изменив графики зарядки электромобилей. Атака разворачивается в несколько этапов: во-первых, злоумышленник находит EVCS с помощью таких инструментов, как Shodan[1] и Censys[2], получая доступ к IP-адресам и портам. Затем, используя слабые места в системе безопасности, такие как стандартные имена пользователей и пароли, найденные в руководствах производителя, злоумышленник получает контроль над EVCS. Этот контроль позволяет манипулировать расписаниями зарядки электромобилей, перенаправляя зарядный трафик в определенные места и время, что в конечном итоге создает узкое место в электросети. Наконец, злоумышленник инициирует сбои на уровне сети, координируя внезапные всплески спроса на электроэнергию или обращая потоки энергии от электромобилей обратно в сеть. Эти организованные атаки могут привести к нестабильности частоты, прогрессирующим сбоям и дисбалансу между спросом и предложением электроэнергии.

Существует несколько других атак, таких как FDI (*False Data Injection*), когда злоумышленники манипулируют передачей данных между EVSE и системами управления, что приводит к перезарядке аккумуляторов или нарушению стабильности сети [26].

Внедрение вредоносного ПО может быть нацелено именно на общедоступные устройства EVSE, что может скомпрометировать всю экосистему EVCS, включая CMS и электросеть [26].

В работе [25] описаны атаки SQL-инъекций на базы данных в EVCS, которые влияют на способность пользователей заряжаться, на данные о местоположении зарядной станции или статусе доступности станции, что

[1] Search Engine for the Internet of Everything [Электронный ресурс] // Shodan, 2025. URL: https://www.shodan.io

[2] Censys Search [Электронный ресурс] // Censys, 2025. URL: https://search.censys.io

потенциально может вызвать проблемы с общественной безопасностью.

V. Защита от атак на инфраструктуру зарядки

Чтобы снизить эти риски, крайне важно внедрить комплексные меры кибербезопасности в EVCI. Процитированная выше работа [27], описывала атаки на EVCI согласно предложенному компанией Майкрософт фреймворку STRIDE, который помогает выявлять (точнее – систематизировать) потенциальные риски безопасности и уязвимости в EVCS на ранних этапах разработки. STRIDE – это аббревиатура, составленная по первым буквам названий 6 угроз: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege.

Шесть угроз, описанных в STRIDE, включают спуфинг, когда злоумышленники выдают себя за авторизованные источники для установки вредоносного ПО на зарядные устройства, что может привести к отключению станций; вмешательство, включающее введение ложных данных о зарядке, которые могут ввести в заблуждение работу сети или повредить электромобили; отказ в работе, когда скомпрометированные зарядные устройства отказываются обрабатывать плату за зарядку, даже если владелец электромобиля уже заплатил за нее, что приводит к финансовым потерям для владельца электромобиля; раскрытие информации (утечка данных), делающее конфиденциальную связь между зарядными устройствами и транспортными средствами доступной для несанкционированного перехвата; DoS-атаки, которые могут наводнить сеть и вывести из строя услуги тарификации; подъем привилегий, где злоумышленники получают несанкционированный доступ к критически важным данным и изменяют системные файлы, чтобы нарушить работу всей сети зарядки.

Пример использования этой модели есть в работе [32]. Решение носит модельный характер для CPS, так что можно рассмотреть его подробнее. Общая схема работы представлена на рисунке 8.

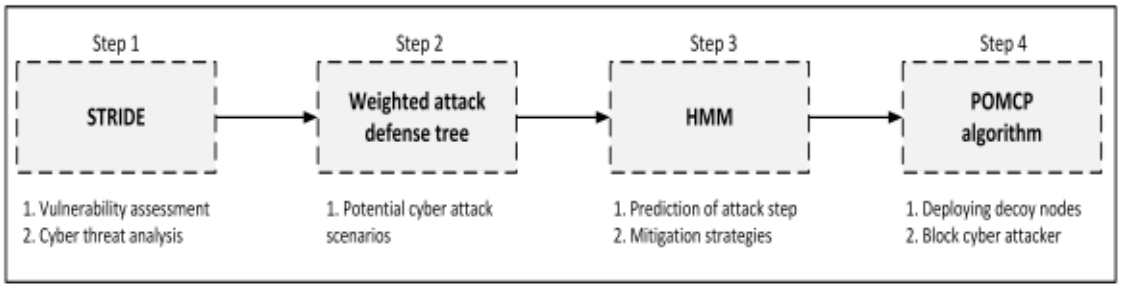

Рис. 8. Модель обеспечения безопасности для CPS [32]

На первом шаге описываются угрозы, исходя из классификации STRIDE для конкретной системы[3]. На шаге 2 строится так называемое взвешенное дерево защиты от атак – это описание различных моделей атак, которые могут быть использованы в конкретной системе. Можно сказать, что это конкретизация рисунка 5 (см. выше) для конкретной системы. В дереве (графе) описываются шаги атаки [33]. На шаге 3 используется скрытая марковская модель (*Hidden Markov Model – HMM*) для прогнозирования шагов атаки с помощью алгоритма Витерби. И, наконец, на шаге 4 используется алгоритм POMCP (*Partially Observable Monte-Carlo Planning*), где добавляются узлы-приманки, чтобы обмануть злоумышленника.

Предлагаемое взвешенное дерево защиты от атак, показанное на рис. 9, анализирует цели атаки противника, демонстрируя графическую древовидную нотацию в форме многоуровневого иерархического процесса. Корневой узел (L1: атака EVCS) дерева атаки определяет основную цель злоумышленника, которая может быть достигнута с помощью различных комбинаций шагов атаки (или подцелей, т. е. L2-2, L2-3, L2-4). Каждый лист атаки может составлять один или несколько узлов защиты и логических узлов “И” и “ИЛИ”. Например, злоумышленник может достичь цели группы L2-3 по отключению EVC с помощью различных сценариев кибератаки. Один из сценариев (т. е. L3-2) – DoS-атака на зарядное устройство. Агент может достичь своей цели, атакуя через два разных сценария атаки или пути, например, используя атаку на пропускную способность сети (NB) (L4-1) и атаку истощения системных ресурсов (SR) (L4-2).

NB имеет три условия “И”, то есть:

(1) сетевой флуд (NF) и некорректный пакет (M),
(2) M и эксплуатация уязвимости протокола (P),
(3) P и усиление (A) атаки.

SR имеет три условия “И”, то есть:

(1) множественные попытки входа в систему (ML) и модификация файловой системы (FM),
(2) FM и установка вредоносного ПО (MI),
(3) MI и флуд приложения (AF).

[3] The STRIDE Threat Model [Электронный ресурс] // Microsoft, Dec. 2009. URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

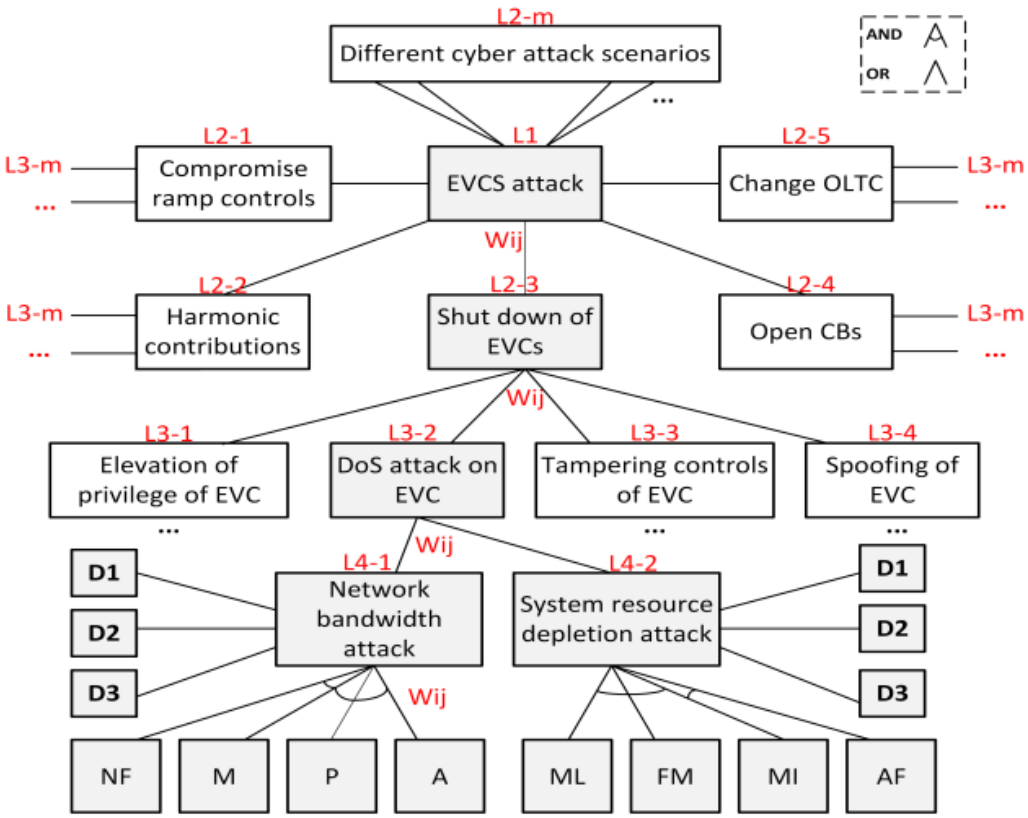

Рис. 9. Дерево DoS атаки [32]

Дерево атак также предлагает несколько действий по смягчению последствий для каждого сценария атаки (L4-1 и L4-2) для стратегий защиты. D1, D2, D3 – защитные узлы. Wij, весовой коэффициент, используется для оценки стоимости защиты (оператором) или стоимости атаки (атакующим). Он также учитывает другие основные факторы, например, стоимость защиты Cij для разработки оборонительных стратегий в CPS [34].

Первая линия защиты в EVCI включает в себя защиту сетей с помощью межсетевых экранов и фильтрацию соединений из надежных источников, а также внедрение надежных протоколов аутентификации. Эти меры предназначены для предотвращения распространенных эксплойтов и защиты от основных попыток несанкционированного доступа. После этих начальных шагов может быть введен дополнительный уровень безопасности для мониторинга необычной активности. Этим занимаются системы обнаружения вторжений IDS/NIDS [35], поскольку они постоянно отслеживают трафик данных и взаимодействие с пользователями, такие как графики зарядки, выявляя и реагируя на любые отклонения от обычных шаблонов.

IDS используют различные подходы, основанные на источнике информации и стратегиях анализа, для защиты от киберугроз. IDS на основе узлов развертываются на отдельных узлах с использованием системных журналов, журналов приложений и журналов аудита для мониторинга и реагирования на вредоносные действия, непосредственно влияющие на систему. Эти IDS сосредоточены на обнаружении несанкционированного доступа, подделки файлов и неправомерного использования ресурсов путем анализа данных от брандмауэров, маршрутизаторов и операционных систем. И наоборот, сетевые IDS отслеживают весь сетевой трафик для выявления потенциальных угроз, затрагивающих несколько систем [36]. Отметим также, что модели IDS – одна из самых частых мишеней в атаках на модели машинного обучения [37].

В работе [17], многократно цитированной в этой статье предлагается размещение системы IDS непосредственно в электромобиле.

Интеграция IDS на основе хоста непосредственно в электромобили обеспечивает критически важную защиту от конкретных угроз в точке взаимодействия между электромобилем и зарядной станцией, таких как фальшивые данные (FDI) и спуфинг. Оснащение электромобилей надежной системой идентификации на основе хоста позволяет создать комплексный механизм защиты, который не только защищает системы автомобиля, но и обеспечивает взаимодействие с данными во время процесса зарядки. Этот подход имеет решающее значение для поддержания целостности и безопасности электромобиля в более широкой экосистеме EVCI.

Учитывая, что потребление энергии и срок службы батареи являются серьезными проблемами в электромобилях, TinyML [38] становится эффективным инструментом для внедрения IDS в эти транспортные средства. Ключевым преимуществом TinyML является его способность проводить обнаружение аномалий в

режиме реального времени непосредственно на микроконтроллерах, встроенных в электромобили. Обрабатывая данные локально на этих устройствах, значительно снижается риск перехвата данных и несанкционированного доступа. Такой локализованный подход не только повышает безопасность, но и согласуется с целями устойчивого развития по сокращению общего потребления энергии в электромобилях. Для этой цели модель машинного обучения должна быть оптимизирована и развернута для вывода на периферийном устройстве, которое в данном случае относится к микроконтроллеру в электроавтомобиле. Микроконтроллер, предназначенный для целей IDS, устанавливается внутри электромобиля для мониторинга CAN-шины. Этот мониторинг имеет решающее значение, поскольку CAN-шина служит каналом для всех оперативных данных, управляя различными функциями, включая взаимодействие с EVCS. Изучая трафик и коммуникации на предмет аномалий, система выявляет потенциальные атаки, которые могут обойти традиционные меры безопасности, такие как брандмауэры. Он обнаруживает необычные или вредоносные действия, в том числе от скомпрометированных зарядных станций или неправильных данных о зарядке, которые могут поставить под угрозу работу автомобиля.

VI. Заключение

В настоящей статье представлен обзор известных (описанных в литературе) кибератак на системы (инфраструктуру) зарядки электротранспорта. Рассмотренные примеры атак, равно как и представленные подходы к защите являются типичными для киберфизических систем. Соответственно, представленные материалы могут быть обобщены и на другие подобные системы. Материалы статьи использованы в учебном курсе “Безопасность инфраструктурных технологий” на факультете вычислительной математики и кибернетики МГУ имени М. В. Ломоносова в рамках реализации совместной магистерской программы “Кибербезопасность” с ПАО Сбербанк.

Благодарности

Авторы благодарны коллективу кафедры информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова за создание благоприятной научной атмосферы, плодотворные дискуссии и конструктивные замечания.

Библиография

[1] Стулов, М. Количество зарядок для электромобилей в Москве вырастет на 11000 // Ведомости, 23 окт. 2023. https://www.vedomosti.ru/gorod/smartcity/articles/kolichestvo-zaryadok-dlya-elektromobilei-v-moskve-virastet-na-11-000. Retrieved: Jan, 2025

[2] Outlook for electric vehicle charging infrastructure // Global EV Outlook 2024. Paris: IEA, 2024. https://www.iea.org/reports/global-ev-outlook-2024/outlook-for-electric-vehicle-charging-infrastructure. Retrieved: Jan, 2025

[3] Бабаян, Г. В. Анализ влияния инфраструктуры электрозаправок на массовое внедрение электромобилей в крупных городах США и Европы // Universum: технические науки. – 2024. – № 10-3(127). – С. 52-63. – EDN: GDEFQX

[4] Electric Vehicle Range Anxiety: An Obstacle for the Personal Transportation (R)evolution? / D. Pevec, J. Babic [et al.] // 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech). – Split, Croatia: IEEE Press, 2019. – P. 1-8. doi: 10.23919/SpliTech.2019.8783178.

[5] Критическая информационная инфраструктура России // TAdviser, 2025. https://www.tadviser.ru/index.php/Статья:Критическая_информационная_инфраструктура_России. Retrieved: Jan, 2025

[6] Eisel, M., Schmidt, J., Kolbe, L. M. Finding suitable locations for charging stations // 2014 IEEE International Electric Vehicle Conference (IEVC). – Florence, Italy: IEEE Press, 2014. – P. 1-8. doi: 10.1109/IEVC.2014.7056134.

[7] Bhat, F. A., Tiwari, G. Y., Verma, A. Preferences for public electric vehicle charging infrastructure locations: A discrete choice analysis // Transport Policy. – 2024. – Vol. 149. – P. 177-197. doi: 10.1016/j.tranpol.2024.02.004.

[8] Scoblete, G. Electric Vehicles in Focus, Part V: The Evolving Cyber Threat to EV Charging Stations // Verisk Analytics, Sep. 2023. https://core.verisk.com/Insights/Emerging-Issues/Articles/2023/September/Week-4/The-Cyber-Risks-of-Electric-Vehicle-Charging-Stations. Retrieved: Jan, 2025

[9] Isle of Wight: Council's electric vehicle chargers hacked to show porn site, https://www.bbc.com/news/uk-england-hampshire-61006816. Retrieved: Jan, 2025

[10] Schwartz, M. J. Electric Vehicle Charging Stations at Risk From Hack Attacks // ISMG, Oct. 2024. https://www.bankinfosecurity.com/electric-vehicle-charging-stations-at-risk-from-hack-attacks-a-26620. Retrieved: Jan, 2025

[11] Jeong, S. I., Choi, D.-H. Electric Vehicle User Data-Induced Cyber Attack on Electric Vehicle Charging Station // IEEE Access. – 2022. – Vol. 10. – P. 55856-55867. doi: 10.1109/ACCESS.2022.3177842.

[12] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D. and Douligeris, C. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP) // IEEE Communications Surveys & Tutorials. – 2022. – Vol. 24, no. 3. – P. 1504-1533. doi: 10.1109/COMST.2022.3184448.

[13] Магистратура “Кибербезопасность МГУ-СБЕР” // ВМК МГУ имени М.В. Ломоносова, 2025. https://cyber.cs.msu.ru. Retrieved: Jan, 2025

[14] Намиот, Д. Е., Сухомлин, В. А. О кибербезопасности систем Интернета Вещей // International Journal of Open Information Technologies. – 2023. – Т. 11, № 2. – С. 85-97. – EDN: DCDCHM

[15] Namiot, D. E., Sneps-Sneppe, M., Daradkeh, Y. I. On internet of things education // 2017 20th Conference of Open Innovations Association (FRUCT). – St. Petersburg, Russia: IEEE Press, 2017. – P. 309-315. doi: 10.23919/FRUCT.2017.8071327.

[16] Sarieddine, K., Sayed, M. A., Torabi, S., Atallah, R., Assi, C. Investigating the Security of EV Charging Mobile Applications as an Attack Surface // ACM Transactions on Cyber-Physical Systems. – 2023. – Vol. 7, no. 4. – Art. no. 26. doi: 10.1145/3609508.

[17] Dehrouyeh, F., Yang, L., Badrkhani Ajaei F., Shami, A. On TinyML and Cybersecurity: Electric Vehicle Charging Infrastructure Use Case // IEEE Access. – 2024. – Vol. 12. – P. 108703-108730. doi: 10.1109/ACCESS.2024.3437192.

[18] ElHussini, H., Assi, C., Moussa, B., Atallah, R., Ghrayeb, A. A Tale of Two Entities: Contextualizing the Security of Electric Vehicle Charging Stations on the Power Grid // ACM Transactions on Internet of Things. – 2021. – Vol. 2. – Art. no. 8. doi: 10.1145/3437258.

[19] Das, H. S., et al. Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review // Renewable and Sustainable Energy Reviews. – 2020. – Vol. 120. – Art. no. 109618. doi: 10.1016/j.rser.2019.109618.

[20] Metere, R. et al. Securing the Electric Vehicle Charging Infrastructure // arXiv:2105.02905, 2022. doi: 10.48550/arXiv.2105.02905.

[21] Antoun, J., Kabir, M. E., Moussa, B., Atallah, R., Assi, C. A Detailed Security Assessment of the EV Charging Ecosystem // IEEE Network. – 2020. – Vol. 34, no. 3. – P. 200-207. doi: 10.1109/MNET.001.1900348.

[22] Balakrishnan, P. C., Pillai, A. S. Design and development of smart interoperable electric vehicle supply equipment for electric mobility // International Journal of Electrical and Computer Engineering. – 2023. – Vol. 13, no. 3. – P. 3509-3518. doi: 10.11591/ijece.v13i3.pp3509-3518.

[23] Cardenas, A. Cyber-Physical Systems Security Knowledge Area. Version 1.0.1 // The Cyber Security Body Of Knowledge; ed. by E.

Lupu. – The National Cyber Security Centre; 2021. – 61 p. https://www.cybok.org/media/downloads/Cyber_Physical_Systems-v1.0.1.pdf. Retrieved: Jan, 2025
[24] Abu-Nassar, A. M., Morsi, W. G. Early Detection of Cyber-Physical Attacks on Electric Vehicles Fast Charging Stations Using Wavelets and Deep Learning // IEEE Transactions on Industrial Cyber-Physical Systems. – 2024. – Vol. 2. – P. 220-231. doi: 10.1109/TICPS.2024.3413605.
[25] Gottumukkala, R., Merchant, R., Tauzin, A., Leon, K., Roche, A., Darby, P. Cyber-physical System Security of Vehicle Charging Stations // 2019 IEEE Green Technologies Conference (GreenTech). – Lafayette, LA, USA: IEEE Press, 2019. – P. 1-5. doi: 10.1109/GreenTech.2019.8767141.
[26] Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D., Lloret, J. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations // Sensors. – 2023. – Vol. 23, issue 15. – Art. no. 6716. doi: 10.3390/s23156716.
[27] Shirvani, S., Baseri, Y., Ghorbani, A. Evaluation Framework for Electric Vehicle Security Risk Assessment // IEEE Transactions on Intelligent Transportation Systems. – 2024. – Vol. 25, no. 1. – P. 33-56. doi: 10.1109/TITS.2023.3307660.
[28] Basnet, M., Ali, M. H. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning // IET Generation, Transmission & Distribution. – 2021. – Vol. 15, issue 24. – P. 3435-3449. doi: 10.1049/gtd2.12275.
[29] Zhou, Y., et al. Malicious Mode Attack on Electric Vehicle Coordinated Charging and its Defense Strategy // Sustainable Energy, Grids and Networks. – 2024. – Vol. 39. – Art. no. 101440. doi: 10.1016/j.segan.2024.101440.
[30] Liu, W., Li, L., Li, X. Power System Forced Oscillation Caused by Malicious Mode Attack via Coordinated Charging // 2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). – Shanghai, China: IEEE Press, 2022. – P. 1838-1844. doi: 10.1109/ICPSAsia55496.2022.9949689.
[31] Gandhi, K., Morsi, W. G. Impact of the Open Charge Point Protocol Between the Electric Vehicle and the Fast Charging Station on the Cybersecurity of the Smart Grid // 2022 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). – Halifax, NS, Canada: IEEE Press, 2022. – P. 235-240. doi: 10.1109/CCECE49351.2022.9918406.
[32] Girdhar, M., Hong, J., Yoo Y., Song, T.-j. Machine Learning-Enabled Cyber Attack Prediction and Mitigation for EV Charging Stations // 2022 IEEE Power & Energy Society General Meeting (PESGM). – Denver, CO, USA: IEEE Press, 2022. – P. 1-5. doi: 10.1109/PESGM48719.2022.9916914.
[33] Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P. Attack – defense trees // Journal of Logic and Computation. – 2014. – Vol. 24, issue 1. – P. 55-87. doi: 10.1093/logcom/exs029.
[34] Xu, B., Zhong, Z., He, G. A minimum defense cost calculation method for attack defense trees // Security and Communication Networks. – 2020. – Vol. 2020, issue 1. – Art. no. 8870734. doi: 10.1155/2020/8870734.
[35] ElKashlan, M., Aslan, H., Said Elsayed, M., Jurcut, A. D., Azer, M. A. Intrusion Detection for Electric Vehicle Charging Systems (EVCS) // Algorithms. – 2023. – Vol. 16, issue 2. – Art. no. 75. doi: 10.3390/a16020075.
[36] Thakkar, A., Lohiya, R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions // Artificial Intelligence Review. – 2022. – Vol. 55, issue 1. – P. 453-563. doi: 10.1007/s10462-021-10037-9.
[37] Намиот, Д. Е. О кибератаках с помощью систем Искусственного интеллекта // International Journal of Open Information Technologies. 2024. Т. 12, № 9. С. 132-141. EDN: PEEQXY
[38] Elhanashi, A., Dini, P., Saponara, S., Zheng, Q. Advancements in TinyML: Applications, Limitations, and Impact on IoT Devices // Electronics. – 2024. – Vol. 13, issue 17. – Art. no. 3562. doi: 10.3390/electronics13173562.

Об авторах:

Намиот Дмитрий Евгеньевич, ведущий научный сотрудник лаборатории открытых информационных технологий кафедры информационной безопасности факультета вычислительной математики и кибернетики, доктор технических наук, ФГБОУ ВО "Московский государственный университет имени М.В. Ломоносова" (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: https://orcid.org/0000-0002-4463-1678, dnamiot@gmail.com

Пичугов Алексей Александрович, ведущий специалист кафедры информационной безопасности факультета вычислительной математики и кибернетики, ФГБОУ ВО "Московский государственный университет имени М.В. Ломоносова" (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: https://orcid.org/0009-0001-3489-7915, pichugov.a.a@cs.msu.ru

Мякишев Андрей Павлович, руководитель учебного центра, НТЦ "Вулкан" (105318, Российская Федерация, г. Москва, ул. Ибрагимова, д. 31); ведущий специалист кафедры информационной безопасности факультета вычислительной математики и кибернетики, ФГБОУ ВО "Московский государственный университет имени М.В. Ломоносова" (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: https://orcid.org/0009-0003-7448-3930, a.myakishev@ntc-vulkan.ru

On Cyberattacks on Charging Stations

Dmitry Namiot, Alexey Pichugov, Andrey Myakishev

***Abstract*— The share of electric transport in all countries is steadily growing. Charging infrastructure is obviously one of the determining factors for this growth. This infrastructure (its operability) is a critical element for electric cars. And it is this infrastructure that becomes the target of cyberattacks. The main security problem is that when an electric car connects to a charging station, the car and the charging station interact with each other using a network connection. This connection is carried out via the power line of the charging cable. And the modem responsible for this interaction is available as a normal network interface on the charging station controller. Because of this, incorrectly configuring services on the charging station controller (compromising them) can lead to these services being available on the charging cable, which opens up great opportunities for cyberattacks. The desire to ensure convenience and flexibility of the charging process, to a certain extent, conflicts with the need to ensure security. All this has led to more and more examples of cybersecurity issues specifically for charging stations and related infrastructure, which can also be attacked.**

***Keywords*— electric transport, charging, cyberattacks.**

REFERENCES

[1] M. Stulov, "Kolichestvo zarjadok dlja jelektromobilej v Moskve vyrastet na 11000," in: *Vedomosti,* [Online]. 23 Oct. 2023. Available: https://www.vedomosti.ru/gorod/smartcity/articles/kolichestvo-zaryadok-dlya-elektromobilei-v-moskve-virastet-na-11-000. Retrieved: Jan, 2025 (In Russ.)

[2] "Outlook for electric vehicle charging infrastructure," in: *Global EV Outlook 2024*, [Online]. Paris: IEA, 2024. Available: https://www.iea.org/reports/global-ev-outlook-2024/outlook-for-electric-vehicle-charging-infrastructure. Retrieved: Jan, 2025

[3] G. V. Babajan, "Analysis of the impact of electric charging infrastructure on the mass introduction of electric vehicles in major cities in the United States and Europe", *Universum: tehnicheskie nauki,* no. 10-3(127), pp. 52-63, 2024. (In Russ., abstract in Eng.) EDN: GDEFQX

[4] D. Pevec, J. Babic, A. Carvalho, Y. Ghiassi-Farrokhfal, W. Ketter, and V. Podobnik, "Electric Vehicle Range Anxiety: An Obstacle for the Personal Transportation (R)evolution?" in: *2019 4th International Conference on Smart and Sustainable Technologies (SpliTech),* Split, Croatia: IEEE Press, 2019, pp. 1-8, doi: 10.23919/SpliTech.2019.8783178.

[5] "Kriticheskaja informacionnaja infrastruktura Rossii", in: *TAdviser*, [Online]. 2025. Available: https://www.tadviser.ru/index.php/Статья:Критическая_информационная_инфраструктура_России. Retrieved: Jan, 2025 (In Russ.)

[6] M. Eisel, J. Schmidt, and L. M. Kolbe, "Finding suitable locations for charging stations," in: *2014 IEEE International Electric Vehicle Conference (IEVC),* Florence, Italy: IEEE Press, 2014, pp. 1-8, doi: 10.1109/IEVC.2014.7056134.

[7] F.A. Bhat, G.Y. Tiwari, and A. Verma, "Preferences for public electric vehicle charging infrastructure locations: A discrete choice analysis," *Transport Policy,* vol. 149, pp. 177-197, 2024, doi: 10.1016/j.tranpol.2024.02.004.

[8] G. Scoblete, "Electric Vehicles in Focus, Part V: The Evolving Cyber Threat to EV Charging Stations," in: *Verisk Analytics*, [Online]. Sep. 2023. Available: https://core.verisk.com/Insights/Emerging-Issues/Articles/2023/September/Week-4/The-Cyber-Risks-of-Electric-Vehicle-Charging-Stations. Retrieved: Jan, 2025

[9] Isle of Wight: Council's electric vehicle chargers hacked to show porn site. [Online]. Available: https://www.bbc.com/news/uk-england-hampshire-61006816 Retrieved: Jan, 2025

[10] M.J. Schwartz, "Electric Vehicle Charging Stations at Risk From Hack Attacks," *ISMG,* [Online]. Oct. 2024. Available: https://www.bankinfosecurity.com/electric-vehicle-charging-stations-at-risk-from-hack-attacks-a-26620. Retrieved: Jan, 2025

[11] S.I. Jeong and D.-H. Choi, "Electric Vehicle User Data-Induced Cyber Attack on Electric Vehicle Charging Station," *IEEE Access*, vol. 10, pp. 55856-55867, 2022, doi: 10.1109/ACCESS.2022.3177842.

[12] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "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, no. 3, pp. 1504-1533, 2022, doi: 10.1109/COMST.2022.3184448.

[13] Academic Program with Sberbank "Cybersecurity MSU-SBER", in: *Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University*, [Online]. 2025. Available: https://cyber.cs.msu.ru Retrieved: Jan, 2025 (In Russ.)

[14] D.E. Namiot and V.A. Sukhomlin, "On Cybersecurity of the Internet of Things Systems," *International Journal of Open Information Technologies*, vol. 11, no. 2, pp. 85-97, 2023. (In Russ., abstract in Eng.) EDN: DCDCHM

[15] D.E. Namiot, M. Sneps-Sneppe, and Y.I. Daradkeh, "On internet of things education," in: *2017 20th Conference of Open Innovations Association (FRUCT),* St. Petersburg, Russia: IEEE Press, 2017, pp. 309-315, doi: 10.23919/FRUCT.2017.8071327.

[16] K. Sarieddine, M.A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Investigating the Security of EV Charging Mobile Applications as an Attack Surface," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 4, Art. no. 26, 2023, doi: 10.1145/3609508.

[17] F. Dehrouyeh, L. Yang, F. Badrkhani Ajaei, and A. Shami, "On TinyML and Cybersecurity: Electric Vehicle Charging Infrastructure Use Case," *IEEE Access*, vol. 12, pp. 108703-108730, 2024, doi: 10.1109/ACCESS.2024.3437192.

[18] H. ElHussini, C. Assi, B. Moussa, R. Atallah, and A. Ghrayeb, "A Tale of Two Entities: Contextualizing the Security of Electric Vehicle Charging Stations on the Power Grid," *ACM Transactions on Internet of Things*, vol. 2, Art. no. 8, 2021, doi: 10.1145/3437258.

[19] H. S. Das, et al., "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," *Renewable and Sustainable Energy Reviews*, vol. 120, Art. no. 109618, 2020, doi: 10.1016/j.rser.2019.109618.

[20] R. Metere, et al., "Securing the Electric Vehicle Charging Infrastructure," 2022, arXiv:2105.02905, doi: 10.48550/arXiv.2105.02905.

[21] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A Detailed Security Assessment of the EV Charging Ecosystem," *IEEE Network*, vol. 34, no. 3, pp. 200-207, 2020, doi: 10.1109/MNET.001.1900348.

[22] P. C. Balakrishnan, A. S. Pillai, "Design and development of smart interoperable electric vehicle supply equipment for electric mobility," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 3, pp. 3509-3518, 2023. doi: 10.11591/ijece.v13i3.pp3509-3518.

[23] A. Cardenas, "Cyber-Physical Systems Security Knowledge Area. Version 1.0.1," in: *The Cyber Security Body Of Knowledge*. [Online]. E. Lupu, Ed. The National Cyber Security Centre; 2021. 61 p. Available: https://www.cybok.org/media/downloads/Cyber_Physical_Systems-v1.0.1.pdf. Retrieved: Jan, 2025

[24] A. M. Abu-Nassar and W. G. Morsi, "Early Detection of Cyber-Physical Attacks on Electric Vehicles Fast Charging Stations Using Wavelets and Deep Learning," *IEEE Transactions on Industrial Cyber-Physical Systems,* vol. 2, pp. 220-231, 2024, doi: 10.1109/TICPS.2024.3413605.

[25] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical System Security of Vehicle Charging Stations," in: *2019 IEEE Green Technologies Conference(GreenTech),* Lafayette, LA, USA: IEEE Press, 2019, pp. 1-5, doi: 10.1109/GreenTech.2019.8767141.

[26] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown, and J. Lloret, "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations," *Sensors*, vol. 23, issue 15, Art. no. 6716, 2023, doi: 10.3390/s23156716.

[27] S. Shirvani, Y. Baseri, and A. Ghorbani, "Evaluation Framework for Electric Vehicle Security Risk Assessment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 1, pp. 33-56, 2024, doi: 10.1109/TITS.2023.3307660.

[28] M. Basnet and M. H. Ali, "Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning," *IET Generation, Transmission & Distribution*, vol. 15, issue 24, pp. 3435-3449, 2021, doi: 10.1049/gtd2.12275.

[29] Y. Zhou, et al., "Malicious Mode Attack on Electric Vehicle Coordinated Charging and its Defense Strategy," *Sustainable Energy, Grids and Networks*, vol. 39, Art. no. 101440, 2024, doi: 10.1016/j.segan.2024.101440.

[30] W. Liu, L. Li, and X. Li, "Power System Forced Oscillation Caused by Malicious Mode Attack via Coordinated Charging," in: *2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia),* Shanghai, China: IEEE Press, 2022, pp. 1838-1844, doi: 10.1109/ICPSAsia55496.2022.9949689.

[31] K. Gandhi and W. G. Morsi, "Impact of the Open Charge Point Protocol Between the Electric Vehicle and the Fast Charging Station on the Cybersecurity of the Smart Grid," in: *2022 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Halifax, NS, Canada: IEEE Press, 2022, pp. 235-240, doi: 10.1109/CCECE49351.2022.9918406.

[32] M. Girdhar, J. Hong, Y. Yoo, and T. -j. Song, "Machine Learning-Enabled Cyber Attack Prediction and Mitigation for EV Charging Stations," in: *2022 IEEE Power & Energy Society General Meeting (PESGM)*, Denver, CO, USA: IEEE Press, 2022, pp. 1-5, doi: 10.1109/PESGM48719.2022.9916914.

[33] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Attack – defense trees," *Journal of Logic and Computation*, vol. 24, issue 1, pp. 55-87, 2014, doi: 10.1093/logcom/exs029.

[34] B. Xu, Z. Zhong, and G. He, "A minimum defense cost calculation method for attack defense trees," *Security and Communication Networks*, vol. 2020, issue 1, Art. no. 8870734, 2020, doi: 10.1155/2020/8870734.

[35] M. ElKashlan, H. Aslan, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Intrusion Detection for Electric Vehicle Charging Systems (EVCS)," *Algorithms*, vol. 16, issue 2, Art. no. 75, 2023, doi: 10.3390/a16020075.

[36] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review*, vol. 55, issue 1, pp. 453-563, 2022, doi: 10.1007/s10462-021-10037-9.

[37] D. E. Namiot, "On Cyberattacks Using Artificial Intelligence Systems," *International Journal of Open Information Technologies*, vol. 12, no. 9, pp. 132-141, 2024. (In Russ., abstract in Eng.) EDN: PEEQXY

[38] A. Elhanashi, P. Dini, S. Saponara, Q. Zheng, "Advancements in TinyML: Applications, Limitations, and Impact on IoT Devices," *Electronics*, vol. 13, issue 17, Art. no. 3562, 2024, doi: 10.3390/electronics13173562.

About the authors:

Dmitry E. Namiot, Leading Researcher of the Open Information Technologies Lab, Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Dr. Sci. (Eng.), Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: https://orcid.org/0000-0002-4463-1678, dnamiot@gmail.com

Alexey A. Pichugov, Leading Specialist of the Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: https://orcid.org/0009-0001-3489-7915, pichugov.a.a@cs.msu.ru

Andrey P. Myakishev, Head of the Educational center, VULKAN R&D CENTER LLC (31 Ibragimova St., Moscow 105318, Russian Federation); Leading Specialist of the Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: https://orcid.org/0009-0003-7448-3930, a.myakishev@ntc-vulkan.ru