DOI **10.37882/2223–2966.2023.02–2.35**

ПРОГНОЗЫ, ПРОБЛЕМЫ И ПРИОРИТЕТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УЧЕТА ЭНЕРГОРЕСУРСОВ

FORECASTS, PROBLEMS AND PRIORITIES OF ENSURING CYBER SECURITY OF INTELLECTUAL ENERGY ACCOUNTING SYSTEMS

S. Toschuk

Summary. The article is devoted to a detailed study of current problems related to the safe use of intelligent energy accounting systems. A separate emphasis in the research process is made on the problems of protecting "smart" meters. It also highlights the safety priorities that utilities should adhere to when using smart meters. A promising solution to these problems is the introduction of a security approach based on the life cycle of a smart meter, from its production to commissioning and regular use.

Keywords: security, smart meter, threat, data, consumer.

Тощук Сергей Николаевич
Аспирант, Ростовский государственный экономический университета «РИНХ», г. Ростов-на-Дону
toshchuk@yandex.ru

Аннотация. Статья посвящена детальному изучению актуальных на сегодняшний день проблем, связанных с безопасным использованием интеллектуальных систем учета энергоресурсов. Отдельный акцент в процессе исследования сделан на проблемах защиты «умных» счетчиков. Также выделены приоритеты безопасности, которых следует придерживаться коммунальным предприятиям при использовании интеллектуальных счетчиков. Перспективным решением обозначенных проблем является внедрение подхода к безопасности, основанного на жизненном цикле «умного» счетчика, начиная с его производства и заканчивая вводом в эксплуатацию и регулярным использованием.

Ключевые слова: безопасность, «умный» счетчик, угроза, данные, потребитель.

В последнее время в современной энергетике активное развитие приобрело направление Smart Grid. Концепция Smart Grid заключается в том, чтобы сделать «интеллектуальными» генерацию, передачу и распределение электрической энергии благодаря внедрению в электрические сети современных средств диагностики, электронных систем управления и учета, алгоритмов, ограничителей токов короткого замыкания сверхпроводящих линий и других автоматически регулируемых технических процессов [1] .

Одним из основных элементов Smart Grid являются умные счетчики. Эти устройства, подключенные к Интернету, поддерживают двустороннюю связь с другим оборудованием в структуре Smart Grid, что позволяет осуществлять удаленное считывание данных и обслуживание сетей. Прогнозируется, что к 2024 году рынок смарт-счетчиков будет стоить 12 миллиардов долларов, а количество установленных приборов достигнет отметки 1,2 млрд. [2]

Инфраструктура интеллектуальных систем учета энергоресурсов может помочь в борьбе с изменением климата, одновременно обеспечивая экономию для потребителей. Для поставщиков коммунальных услуг интеллектуальные счетчики дают доступ к ценным данным и позволяют разрабатывать дополнительные предложения, которые защищают доходы, дифференцируют услуги и снижают отток клиентов, одновременно сокращая операционные затраты и улучшая управление сетью. Кроме того, интеллектуальные счетчики дают возможность сократить потребление энергии, отходы и выбросы, а также могут стать одним из основополагающих факторов для будущих интеллектуальных сетей, где большие колебания в поставках будут неизбежным параметром [3] .

Обобщая вышеизложенное, можно отметить, что внедрение технологии интеллектуальных сетей и систем учета энергоресурсов, с одной стороны, упрощает и ускоряет управление энергетикой, но, с другой стороны, открывает доступ к возможным кибератакам и неправомерному использованию данных. Как и любое другое устройство, подключенное к сети, интеллектуальные счетчики становятся уязвимыми для атак с разными целями, например, для кражи данных или изменения показаний. В некоторых странах уже произошли взломы умных счетчиков, и потенциальные угрозы огромны — начиная, от испорченной репутации бренда до мошенничества с выставлением счетов и, в конечном итоге, сбоев в подаче электроэнергии.

В данном контексте интеллектуальные сети и все их элементы считаются критически важными инфраструктурами, и, следовательно, предотвращение атак является первоочередной задачей. В апреле 2019 года Европейская комиссия опубликовала Рекомендацию 2019/553 в отношении информационной безопасности применительно к энергетическому сектору [4]. Учитывая высокую степень взаимосвязанности энергетических систем, эта рекомендация призывает работать над разработкой новых стратегий, чтобы избежать вредоносных атак, которые могут привести к серьезным последствиям.

В большинстве случаев системы кибербезопасности интеллектуальных систем учета энергоресурсов основываются на стратегии, известной как цикл PDCA (он также известен как спираль непрерывного совершенствования или цикл Деминга), это четырехступенчатая циклическая основа (Plan, Do, Check and Act), которая ведет к постоянному совершенствованию управления информацией, стандартизированная в серии ISO 27000. Некоторые эксперты считают, что интеллектуальные счетчики могут быть защищены путем адаптации уже существующих методов защиты информации, однако это может создать брешь в системе безопасности [5].

Учитывая отсутствие единого решения для обеспечения защиты и целостности данных интеллектуальных систем учета энергоресурсов, актуальным научно-практическим заданием на сегодняшний день является исследование перспективных и действенных направлений и методов обеспечения защиты данных, конфиденциальности и безопасности при внедрении «умных» счетчиков, что и обуславливает выбор темы данной статьи.

В последнее время проблемные вопросы развития и управления сетями Smart Grid, а также всеми элементами критической инфраструктуры на научном уровне исследовали такие специалисты, как: Потапов В.С., Сопильняк К.В., Xia Zhuoqun, Zhang Yichao, Li Xiong, Jia Weijia.

Теоретические и методические основы обеспечения кибербезопасности в целом нашли свое отражение в работах Ковалева О.Г., Скипидарова А.А., Байгутлиной И.А., Замятина П.А., Olakanmi Oladayo Olufemi, Odeyemi Kehinde Oluwasesan, Wang Rui, Gong Qiujing, Zhen Ke.

Ключевые атрибуты интеллектуальных электрических сетей, а также требования, которые должна реализовывать система защиты изучаются Колосок И.Н., Гуриной Л.А., Петренко С.А., Ступиным Д.Д., Mariana Hentea, M. Kathiresh, A. Mahaboob Subahani.

Вопросы оценки рисков кибербезопасности информационных систем Smart Grid исследовались Стенниковым В.А., Головщиковым В.О., Папковым Б.В., Куликовым А.Л., Осокиным В.Л., Sikdar Biplab, Gope Prosanta, Philips Anita, Jayaraj Jayakumar.

Однако, несмотря на имеющиеся публикации и наработки, проблема обеспечения надежной защиты интеллектуальных счетчиков еще далека от своего решения. Особого внимания заслуживает критический анализ стандартов по информационной безопасности и определение того, какие из них могут быть применены к оценке кибербезопасности «интеллектуальной сети». Также в дополнительном исследовании нуждаются вопросы обоснования наиболее эффективных методов оценки защиты информационных систем Smart Grid.

Таким образом, учитывая вышеприведенные обстоятельства, цель статьи заключается в рассмотрении прогнозов, проблем и приоритетов обеспечения кибербезопасности интеллектуальных систем учета энергоресурсов.

Угрозы кибербезопасности могут принимать различные формы на протяжении всего срока службы интеллектуального счетчика. Взаимосвязь счетчика с Интернетом подвергает сеть новым типам рисков, включая расширенные постоянные угрозы (APT), распределенное-запрещенное обслуживание (DDoS), ботнеты и нулевые дни, Stuxnet, Duqu, Red October или Black Energy — это лишь несколько примеров современных угроз, появившихся буквально за последние годы. Поэтому пользователи «умных» счётчиков должны учитывать различные факторы и быть готовыми к различным векторам атак, чтобы обеспечить защиту своих данных и устройств.

Например, атака по побочному каналу включает в себя прослушивание и анализ потребляемых данных с помощью корреляционного анализа мощности (CPA) для получения учетных данных и доступа к инфраструктуре. Поставщикам энергии и производителям оригинального оборудования (OEM) необходимо обеспечить безопасность от устройства до облака [6]. Также им следует иметь возможность обновлять прошивку по воздуху (OTA) для обеспечения отказоустойчивости в течение всего жизненного цикла устройства.

Учитывая вышеизложенное, не подлежит сомнению тот факт, что внедрение интеллектуальных счетчиков требует мультидисциплинарного подхода, объединяющего различные технологии защиты. Решающую часть этого процесса формирует оценка безопасности, то есть оценка уровня безопасности и выявление потен-

циальных уязвимых мест, которыми могут воспользоваться злоумышленники.

Итак, рассмотрим более подробно проблемы обеспечения кибербезопасности интеллектуальных систем учета энергоресурсов.

Как свидетельствуют вышеприведенные данные, проблем очень много, но большинство из них для интеллектуальной сети можно отнести к одной из двух больших категорий.

Первая категория — это индивидуальные угрозы. В этом случае злоумышленник стремится манипулировать данными интеллектуальной сети для собственной выгоды — возможно, чтобы снизить счет за электроэнергию или скрыть незаконное производство каких-либо товаров, сырья. Индивидуальная угроза не стремится нарушить управление электросетью для других, а только улучшить положение отдельного человека или группы.

Вторая категория — угроза обществу — включает действия, которые пытаются нанести ущерб работе электрической сети. Это может быть атака на само предприятие (массовое занижение данных о потреблении энергии всей сетью может привести к финансовой неустойчивости) или на общество в целом. Ярким примером является террористическая атака, в результате которой электросеть выходит из строя, а потребители остаются без электричества. Без электричества производительность и финансовые потери будут критическими, а в условиях экстремальной жары или холода существует реальная угроза для жизни людей.

Для реализации обозначенных угроз злоумышленник должен найти слабое звено. Атакующий будет рассматривать всю сеть и пытаться определить лучшее место для атаки: где атака принесет желаемый результат с наименьшими инвестициями и риском для атакующего. Рассмотрим простую модель «утилита — конечная точка» для обоих сценариев угроз, чтобы определить, как злоумышленник может достичь своих целей.

Индивидуальная угроза. На примере хакера, который хочет уменьшить свой счет за электричество, злоумышленник может достичь своей цели, проникнув в диспетчерскую и изменив записи, собранные со счетчика. Он также может перехватить связь, передающую информацию о потреблении электроэнергии в коммунальную службу, или же изменить микропрограмму своего счетчика, чтобы занизить данные о количестве потребленной энергии.

Угроза обществу. На примере террориста, который хочет нарушить подачу электроэнергии максимальному количеству пользователей, злоумышленник может проникнуть в диспетчерскую коммунального предприятия и приказать дистанционно отключить ряд счетчиков или прекратить подачу электроэнергии на определенных подстанциях. Преступник также может ввести инструкции в коммуникационную шину, чтобы отдать команду сделать то же самое. Также он может взять под контроль счетчики и запрограммировать их непосредственно на активацию реле дистанционного отключения, или взять под контроль датчики, чтобы передать ложные данные коммунальным службам, заставив их поверить в необходимость отключения определенных сегментов сети.

Чтобы обеспечить кибербезопасность интеллектуальных систем учета энергоресурсов коммунальные службы должны принять во внимание ряд приоритетов безопасности, защиты данных и конфиденциальности, которые включают в себя:

- защиту целостности устройства на территории потребителя — гарантия того, что программное обеспечение не будет подделано;
- доказательство и защиту целостности происхождения данных, передаваемых между потребителем и коммунальным предприятием;
- аутентификация личности сторон в коммуникации;
- защиту данных от несанкционированного доступа при передаче между помещениями потребителя и поставщиком коммунальных услуг;
- обеспечение нормативного соответствия доступа к данным при их хранении у поставщика коммунальных услуг.

Для устранения проблем и угроз безопасности интеллектуальных счетчиков, по мнению автора, целесообразно использовать подход, основанный на жизненном цикле, начиная с их производства и заканчивая вводом в эксплуатацию и регулярным использованием (рис. 1) .

Теперь рассмотрим способы, предполагающие использование платформы IoT, которая позволит удовлетворить требования безопасности жизненного цикла, играющие решающее значение для обеспечения конфиденциальности интеллектуальных систем учета энергоресурсов.

1. Обеспечение корня доверия для развертывания интеллектуальных счетчиков в масштабе фабрики во время их изготовления. Производственные предприятия, которым поручен выпуск интеллектуальных счетчиков, должны обеспечить баланс между масштабируемостью и устойчивостью, чтобы устройство пользовалось доверием и обеспечивало надежную основу для работы счетчика в полевых условиях.

Рис. 1. Пример жизненного цикла безопасной работы интеллектуального счетчика

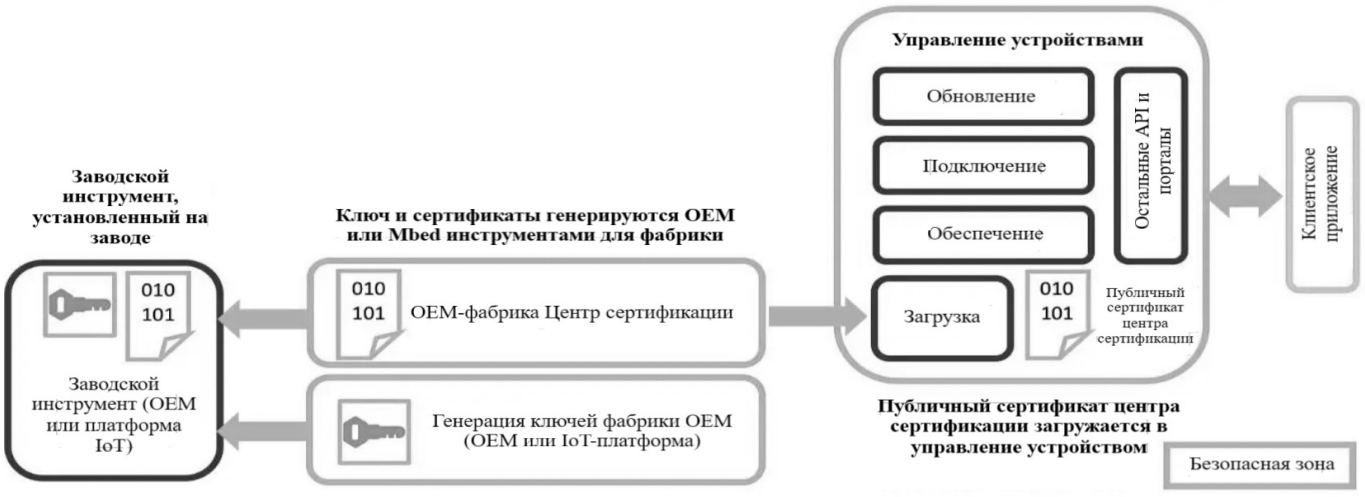

Рис. 2. Пример безопасной производственной линии изготовления «умного» счетчика

Корень доверия (ROT) представляет собой ряд функций в безопасном контуре, которому доверяет операционная система интеллектуального счетчика. Ввод учетных данных в одно устройство может снизить этот риск, но способность масштабировать этот процесс на миллионы устройств является ключевым фактором для поддержания баланса между эффективностью и безопасностью. Вопрос доверия фабрике становится еще более актуальным, если учесть, что коммунальные компании сами не являются производителями и часто передают производство на аутсорсинг OEM-производителям.

В данном случае доверие обеспечивается путем администрирования сертифицирующих центров, которые ссылаются на платформу IoT, загрузочный модуль и легкие серверы M2M (LwM2M). Ряд инструментов, предоставляемых поставщиком платформы IoT, предлагает линейный процесс настройки центра сертификации (ЦС), который гарантирует, что только счетчики, обладающие сертификатом, подписанным ЦС, и открытым ключом, могут установить соединение между устройством и его менеджером устройств. На рис. 2 представлен пример безопасного производства интеллектуального счетчика.

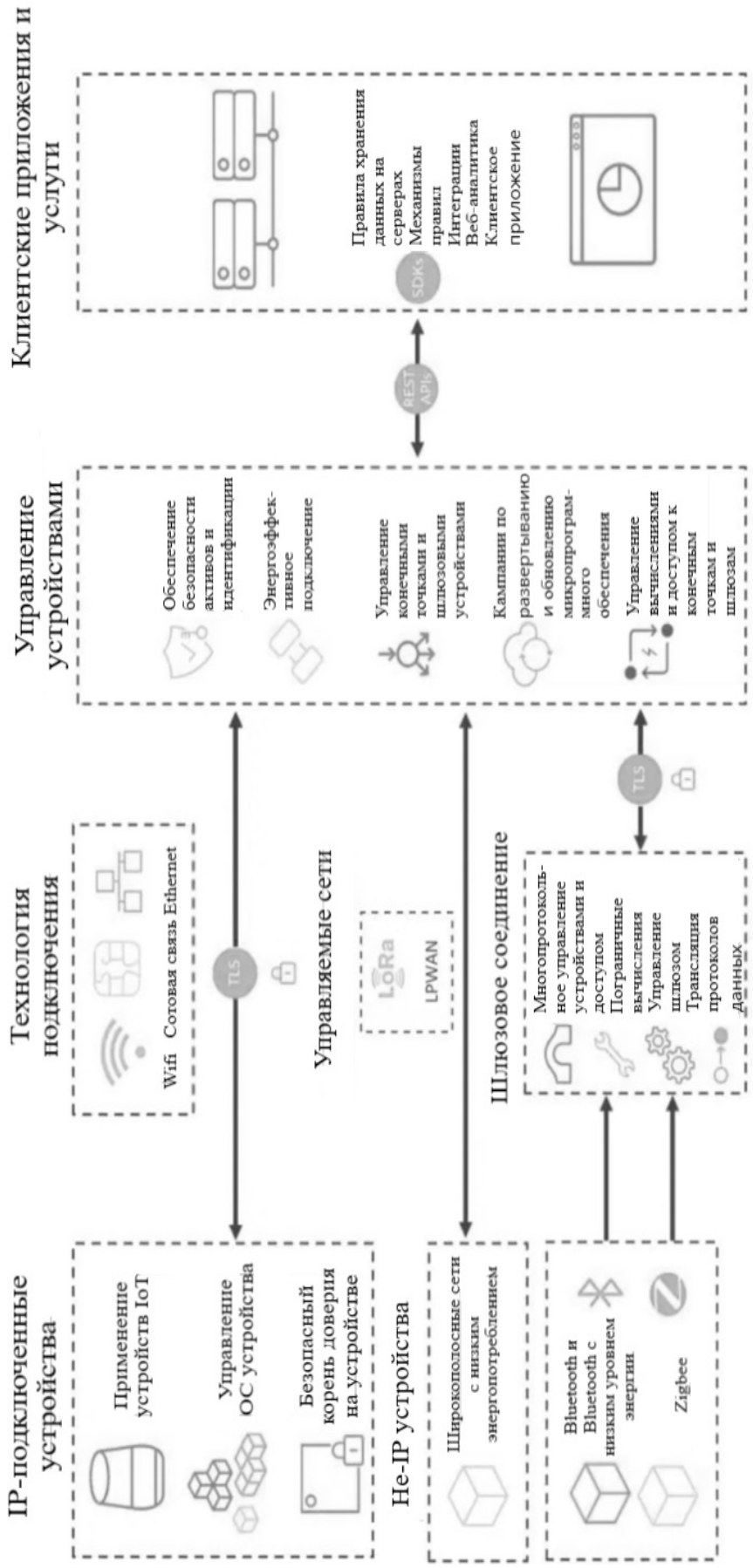

Рис. 3. Пример шифрования TLS от чипа к облаку

После того как ЦС настроен и связан с индивидуальной учетной записью производителя, заводская линия готова к массовому предоставлению устройств. Этот пятиэтапный процесс включает в себя: введение образа программного обеспечения; генерацию ключей устройства, сертификатов и параметров конфигурации; использование заводского инструмента для введения сгенерированных ключей, сертификатов и параметров конфигурации в устройство на производственной линии; применение менеджера конфигурации ключей и клиентского API фабричного конфигуратора (FCC) в устройстве для проверки информации; завершение процесса инициализации и блокировка кода FCC в производственном образе для обеспечения невозможности доступа к нему после инициализации.

2. Надежное соединение с сетью во время ввода в эксплуатацию. Поскольку на этапе производства производитель не имеет представления о том, где будет установлен интеллектуальный счетчик или с каким устройством он будет связан, очень важно, чтобы конечное соединение с сетью было надежным. Поэтому производителям и коммунальным компаниям следует использовать предварительные ключи (PSK), включающие список регистрации. PSK предоставляют как устройствам, так и платформе IoT общий ключ, который был надежно заложен в устройство и является самым базовым уровнем безопасности. Он считается базовым, поскольку существует риск, что учетные данные, переданные интеллектуальному счетчику при производстве, и конфиденциальный список учетных данных, хранящийся на серверах, могут быть скомпрометированы, в результате чего миллионы счетчиков и данные пользователей окажутся незащищенными.

3. Безопасные коммуникации. Внедрение усовершенствованной инфраструктуры учета помогает коммунальным предприятиям автоматизировать мониторинг, выставление счетов, подключение и отключение. Это ожидаемый результат работы интеллектуальных счетчиков, сетей связи и систем управления данными, которые обеспечивают двустороннюю коммуникацию между поставщиками и клиентами. Этот дополнительный уровень связи, поддерживаемый низкой мощностью, дальностью действия и невысокой пропускной способностью, подвергает поставщиков коммунальных услуг дополнительному риску. Поэтому связь между устройством и платформой IoT, а затем веб-приложением поставщика коммунальных услуг должна защищаться с помощью стандарта TLS. На рис. 3 изображен пример шифрования TLS от чипа к облаку.

Таким образом, подводя итоги, отметим, что скорость и масштабы использования интеллектуальных систем учета энергоресурсов открывают значительные возможности для киберпреступников, поскольку вероятность атаки увеличивается с каждым развернутым устройством и каждым установленным обновлением. Для решения проблем с безопасностью целесообразно использовать платформу управления устройствами на базе IoT, которая может помочь создать надежную основу, которая пронизывает весь срок службы счетчика, способствуя оптимизированному масштабируемому развертыванию и обеспечивая защиту как коммунальных предприятий, так и их клиентов.

ЛИТЕРАТУРА

1. Сергиенко В.Г. Концепция интеллектуальных сетей Smart Grid в электроэнергетике // КИП и автоматика: обслуживание и ремонт. 2020. № 8. С. 26–29.
2. Raggi, Livia M.R. Smart Metering in Distribution Systems: Evolution and Applications // Lecture notes in electrical engineering. 2022. Volume 826; pp 287–318.
3. Alemazkoor, Negin Smart-Meter Big Data for Load Forecasting: An Alternative Approach to Clustering // IEEE access: practical innovations, open solutions. 2022. Vol. 10; pp 8377–8387.
4. Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv: OJ.L_. 2019.096.01.0050.01.ENG&toc=OJ: L:2019:096: TOC
5. Xia, Xiaofang Detection Methods in Smart Meters for Electricity Thefts: A Survey // Proceedings of the IEEE. 2022. Volume 110: Number 2; pp 273–319.
6. Kumar, Dharmendra Roll-Out Strategy for Smooth Transition of Traditional Meters to Smart Meters // Lecture notes in electrical engineering. 2022. Volume 764; pp 287–294.

Журнал «Современная наука: актуальные проблемы теории и практики»