



Некоммерческое партнерство  
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ  
Единой энергетической системы»

109044 г.Москва, Воронцовский пер., дом 2  
Тел. (495) 912-1078, 912-5799, факс (495) 632-7285  
E-mail: [dtv@nts-ees.ru](mailto:dtv@nts-ees.ru), <http://www.nts-ees.ru/>  
ИНН 7717150757

«УТВЕРЖДАЮ»

Председатель научно-технической  
коллегии НП «НТС ЕЭС»,  
д.т.н. профессор

Н.Д. Роголев

« 8 » 04 2024г.

## ПРОТОКОЛ

заседания секции «Автоматизированный учет электроэнергии и управление  
электропотреблением» НТС ЕЭС

по теме

Жизненный цикл цифровых решений в электроэнергетике

26.03.2024 г.

№ 22

г. Москва

**Заседание проводилось в комбинированном формате (очно и дистанционно).**

**Присутствовали:** 24 человек (список прилагается)

**На заседании выступили:**

С вступительным словом Александр Васильевич Покатилов - председатель секции «Автоматизированный учет электроэнергии и управление электропотреблением». Александр Васильевич доложил об участии в состоявшемся в конце 2023 года заседании научно-технической комиссии (далее – НТК) по метрологии и измерительной технике Росстандарта. Одним из поднятых на заседании вопросов был вопрос по заправочным станциям для электромобилей. На заседании НТК обратили внимание на актуальность темы, отметили различный подход к нему в разных странах: считать это «Услугой» по обслуживанию электромобиля или коммерческим отпуском энергоресурса. Логичным является последнее предложение, по аналогии с заправкой автомобиля бензином. Но заправка бензином не зависит от скорости заправки (15 минут или 2 часа), а только от объема заправки. В случае заправки электромобиля скорость заправки (ток) играет существенную роль и должна учитываться прибором учета (электросчетчиком постоянного

тока). В США приняли решение несколько лет считать заправку услугой с фиксированной ценой и не применять никаких метрологических правил и норм для таких электрозаправочных станций и хабов, в Германии, наоборот, устанавливают счетчики на каждую станцию. В России массовый выпуск электросчетчиков постоянного тока отсутствует. Решения не применять метрологические нормы нет, законодательство об обязательном учете всех энергоресурсов есть, но, в то же время существующие заправочные станции функционируют без счетчиков электроэнергии. НТК Росстандарта принял рекомендацию о необходимости постановки НИР по этому вопросу.

**С основным докладом «Жизненный цикл цифровых решений в электроэнергетике»** (Приложение 1) выступил Евгений Леонидович Генгринович, АО «ИнфоТеКС».

Евгений Леонидович поделился имеющимся опытом внедрения и эксплуатации цифровых решений в электроэнергетике, начав с некоторых определений. Термин «киберустойчивость» – способность системы в условиях внешних информационных воздействий (будь то злонамеренные воздействия, ошибки персонала, ошибки ПО и т.д.) работать и выполнять свои базовые бизнес-функции. Зачастую путают два термина «цифровизация» и «автоматизация». Цифровизация – это повышение эффективности бизнес-процессов при максимальном использовании современных ИТ-технологий. Практически любой объект электроэнергетики сейчас подходит под определение объекта критической информационной инфраструктуры (далее – КИИ) и основные требования к таким объектам следующие:

- Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры РФ» (далее - №187-ФЗ) и ряд сопутствующих ему приказов ФСТЭК.
- Постановление Правительства РФ от 14 ноября 2023 г. №1912 «О порядке перехода субъектов критической информационной инфраструктуры РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры РФ» (далее – ПП №1912).

С точки зрения бизнеса важны эффективность, доступность и надежность. На все эти требования налагаются процессы цифровой трансформации, когда бизнес-процессы видоизменяются согласно последним достижениям ИТ-технологий. Прямолинейно выполняя все требования законодательства стоимость любой системы управления информационной безопасностью будет являться серьезной финансовой нагрузкой, которую зачастую пытаются минимизировать или даже избежать. Если же взглянуть на ситуацию с

точки зрения бизнеса, то стоит изначально (заранее) обратить внимание на киберустойчивость внедряемых решений, таким образом, как не удивительно, можно получить решение, соответствующее требованиям государства, за гораздо меньшие деньги.

Более детальное рассмотрение требований законодательства, а именно №187-ФЗ Статья 2 п.2 - безопасность КИИ - состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак. Приведенное определение схоже с ранее приведенным определением киберустойчивости. То есть, даже в ФЗ речь идет не о безопасности как таковой, а об устойчивом функционировании технологических процессов, которые мы защищаем. Второй документ, ПП №1912, касается вопросов, связанных с импортозамещением. Определяется, что до 2030 года должно быть проведено импортозамещение на всех объектах КИИ на «доверенные ПАК» (впервые введенный термин). ПАК является доверенным, в том числе, в случае реализации в нем функций защиты информации, соответствующих требованиям, установленным ФСТЭК и (или) ФСБ, что должно быть подтверждено соответствующим документом.

Киберустойчивость это фактически система управления технологическими рисками. Управлять этими рисками необходимо еще на стадии разработки устройства, а не в период опытно-промышленной эксплуатации. В противном случае, неучтенный риск очень дорого стоит, как для самих разработчиков решения, так и для заказчиков.

Если говорить о неблагоприятных условиях эксплуатации любого объекта, то помимо классических воздействий на него на свежем воздухе (температура, природные катаклизмы, ошибки персонала, производственный брак и т.д.), для современных цифровых устройств появляются информационные воздействия нового поколения - ошибки ПО, ошибки при конфигурировании ПО, отказы сети передачи данных, несанкционированное вмешательство и т.д.

Второй момент, который часто упускают из вида, это поддержка актуальности цифровых документов в эксплуатации. При бумажном документообороте всегда есть возможность обратиться в архив и просмотреть пущую версию документации, в случае электронного документооборота проверить достоверность файла довольно сложно. Например, срок действия электронно-цифровой подписи (далее – ЭЦП) всего 1 год, если документ был подписан 3 года назад, за этот период с ним могло произойти все что угодно, т.к. ЭЦП, поставленная на этот документ уже не действует.

Системы, в отношении киберустойчивости, можно классифицировать следующим образом – уже внедренные системы/ проектируемые в настоящее время (считает, что какие-либо изменения в их компоненты вносить уже проблематично) и вновь создаваемые. Для

существующих систем есть стандартный набор инструментов по киберустойчивости это создание виртуальной инфраструктуры, которая обеспечивает изолированный трафик даже при использовании публичных каналов. В такую виртуальную сеть могут включаться как пользователи, так и различные приборы (IP-камеры, дроны и т.д.). В настоящее время есть как аппаратные средства, так и программные, которые позволяют сделать сеть гибкой.

Говоря о сценариях применения, обратили внимание на интеграцию с контроллерами, программная контейнеризация – стандартные докеровские контейнеры, которые поддерживаются операционными системами, и можно, ничего не меняя на уровне контроллера, встроить дополнительный коммуникационный объект в виде программного клиента. Опыт встраивания есть как с российскими, так и с зарубежными производителями, например, Siemens, Wago, Phoenix Contact. Помимо контейнеризации, есть возможности встраивания непосредственно в Линукс-подобные операционные системы (например, IP-камеры компаний НИЦ Технологии и Випакс).

Отдельная тема – человеческий фактор. Многие вопросы необходимо решать непосредственно на объектах и важно, чтобы работы мобильных бригад так же велась по защищенным каналам (есть соответствующие клиенты для мобильных устройств, планшетов и т.д.). Все возможности, предоставляемые западными мессенджерами (голосовые коммуникации, видеосвязь, отправка текстовых сообщений и файлов и т.д.) есть сегодня и в российском исполнении. Существует возможность выполнять защищенные звонки другим пользователями приложения с высоким качеством. Все данные передаются в зашифрованном виде, минуя промежуточные серверы. Острая проблема – отсутствие контроля подключаемых устройств на объектах (помимо стандартной проверки на вирусы). Сегодня существует комплексное решение защиты конечных точек, можно обеспечить преобразование любого ноутбука в специализированный конфигуратор, когда на нем будут запускаться только конкретные процессы для выполнения predetermined производственных функций. Таким образом, отсекается возможность нецелевого использования устройства, в том числе, возможность осуществления злонамеренных действий даже при физическом нахождении на объекте.

В действительности, обеспечить реальную киберустойчивость можно только на вновь создаваемых цифровых решениях. Согласно международной статистике стоимость исправления ошибок от этапа проектирования устройства до этапа промышленной эксплуатации может варьироваться от 25 \$ до 16000 \$ соответственно (разница в стоимости на несколько порядков). Таким образом учет требований по киберустойчивости становится важным бизнес-фактором, при выборе конкурирующих решений Заказчиком.

На сегодняшний день мы можем защищаться от известных нам угроз (у ФСТЭК даже есть перечень известных сценариев атак на конкретные типы систем), но невозможно предсказать, что произойдет с развитием технологий через 5-7 лет (при сроке эксплуатации устройств 15-25 лет). Возможно, устройства попытаются взломать такими способами, которые сегодня даже нельзя представить.

С 2014 года прошло уже несколько «волн» импортозамещения. После выхода ПП №1912, фактически, стало ясно, что действия, выполненные до 2023 года, были не совсем корректны и необходимо заново проходить этот путь. Технологическая независимость важный параметр, но сам по себе он не обеспечивает киберустойчивость. Совместно с центром НТИ МЭИ консолидировали актуальные задачи для производителей систем АСУ ТП, цифровых систем релейной защиты и т.д. Важно разделять безопасную разработку непосредственно самого программного обеспечения (необходимая база) и задачу по его корректной работе внутри ПАК (что добавляет еще ряд требований). Одно из таких требований - создание (помимо самого оборудования) виртуальных программных симуляторов, которые могли бы имитировать его работу. Это необходимо для тестирования любых изменений, произведенных в процессе эксплуатации, чтобы избежать непредсказуемости того, как изменения отразятся на работающем оборудовании.

В части поддержки киберустойчивости, идут процессы стандартизации. С 2016 года принят ГОСТ по разработке безопасного ПО. Сейчас идет работа по внесению в него актуальных изменений, а также разрабатывают целый ряд дополнительных ГОСТов с более детальным описанием требований к безопасной разработке ПО и его проверкам. В феврале был выпущен Приказ Росстандарта о введении в действие с 01.04.2024 года ГОСТ Р 71252 – 2024 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для промышленных систем». Классическая ЭЦП, принятая в ИТ, занимает сотни Кб, при ее использовании, фактически, служебная часть на порядок будет превышать содержательную часть. Был разработан и описан в Национальном стандарте специальный протокол, который позволяет существенно уменьшить эту нагрузку на канал. На базе этого промышленного протокола уже разработаны СКЗИ, которые могут встраиваться непосредственно в оборудование как низовые устройства в виде ПАК, так и программное обеспечение, которое позволяет обеспечить не только криптографическую защиту, но и систему управления ключами (что существенно повышает киберустойчивость используемых решений).

Теперь предлагаю обсудить инструменты для поддержки киберустойчивости на жизненном цикле цифровых решений. Начнем с Цифровых двойников (ЦД). ЦД – это виртуальная реплика любого устройства. Его функциональность определяется тем, что

именно необходимо предсказывать в отношении киберфизического актива (определить бизнес-задачу). В контексте киберустойчивости, нам интересны две бизнес-задачи:

1. контроль функциональной готовности и надежность киберфизического актива;
2. анализ нейтрализации неблагоприятных внешних воздействий.

Технологии постоянно меняются, однако использовать для их тестирования работающие системы никто не позволит. ЦД на сегодня является необходимым элементом для обеспечения нормального цикла эксплуатации цифровых систем.

Рассмотрим цифровой двойник информационно-коммуникационной сети. Данный киберполигон содержит, в том числе, блок системы управления обучением, где можно задавать различные сценарии и выполнять, как исследовательские работы, так и обучение персонала. Другой вариант ЦД - цифровой двойник энергосистемы, разработанный в Центре НТИ МЭИ – моделирование в реальном времени режимов энергообъектов энергосистем разного уровня.

Другой инструмент поддержки жизненного цикла – прокси-платформа Hauberk Pro, сделанная на базе технологий распределенных реестров и смарт-контрактов. На базе этой платформы совместно с Центром НТИ МЭИ изучался вопрос работы с электронной документацией на всех этапах жизненного цикла. Согласно реестрам, можно отследить каждое изменение, вносимое в документацию в процессе эксплуатации и при необходимости запустить процесс согласования в реальном времени.

В заключении докладчиком было отмечено, что простого решения, обеспечивающего киберустойчивость не существует. Однако, последовательная и комплексная работа от начала разработки цифрового решения до его вывода из эксплуатации позволяет обеспечить необходимый уровень киберустойчивости системы на протяжении всего жизненного цикла.

#### **В обсуждении доклада приняли участие:**

Представители АО «ИнфоТеКС», АО «НТЦ ФСК ЕЭС», ПАО «Мосэнерго», ООО НПП «ЭКРА», члены секции НП «НТС ЕЭС».

Тема цифровых двойников, так же, была затронута на заседании Росстандарта. Речь шла о том, чтобы нормализовать базы данных для их построения. Так как, в настоящее время, параметры для разработки цифровых двойников зачастую берут некорректно (например, из недостоверных источников, имеющих в открытом доступе).

Обсудили этапы жизненного цикла цифровых решений. Отметили важность для цифровых решений этапа корректного вывода из эксплуатации. Необходимо уделять внимание утилизации большого объема информации, чтобы не было утечки.

Отметили, что более корректное название доклада было бы «Киберустойчивость на жизненном цикле цифровых решений», то есть в докладе описано, каким образом на каждом этапе жизненного цикла обеспечивается киберустойчивость, чтобы система работала в заданных для нее параметрах.

Обсудили неразрывность понятий автоматизации и цифровизации в существующей системе управления энергообъектами в целом.

Рассмотрели вопрос конкурентноспособности встраиваемых СКЗИ.

Оценили необходимость ограничений наращивания безопасности и есть ли предел в работе с безопасностью, учитывая то, что обеспечить 100%-ю киберустойчивость практически невозможно. Важно найти правильный баланс в стоимости решений и их эффективности, уделяя должное внимание проработке и оценке рисков.

Установили, что развитие кибербезопасности и развитие облачных хранилищ не разнонаправленные тенденции. Однако, при использовании облачных структур необходимо корректно оценивать риски и их прорабатывать (выполнять резервирование, разносить информацию по разным облакам и т.д.).

**Заслушав выступление и обсуждение секция «Автоматизированный учёт электроэнергии и управление электропотреблением» НТС ЕЭС отметила:**

- ✓ Актуальность рассматриваемых вопросов обеспечения киберустойчивости.
- ✓ Необходимость уделять внимание киберустойчивости уже на этапе разработки цифровых решений. Это не только существенно повысит уровень киберустойчивости, но также существенно снизит уровень затрат на ее обеспечение.
- ✓ Киберустойчивость позволяет системе безостановочно работать и выполнять свои функции в заданных режимах, не смотря на неблагоприятные информационные воздействия.

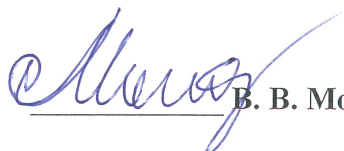
**Секция «Автоматизированный учёт электроэнергии и управление электропотреблением» НТС ЕЭС решила:**

1. Направить материалы состоявшегося заседания и обсуждаемые вопросы в организации-участники секции для использования в работе подразделений информационной безопасности.

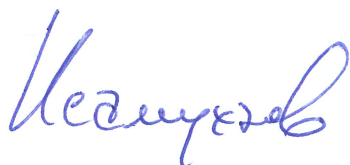
2. Учитывая стремительность развития как аппаратных и программных средств киберустойчивости, так и неблагоприятных информационных воздействий на цифровые системы на всех этапах их жизненного цикла, продолжить периодическое заслушивание докладов по этой тематике.

3. Поручить Председателю секции сделать короткое сообщение об итогах состоявшегося заседания секции на круглом столе Российского международного энергетического форума (РМЭФ-2024) в г. С-Петербурге.

Первый заместитель председателя  
Научно - технической коллегии  
НП «НТС ЕЭС», д.т.н., профессор

  
В. В. Молодюк

Ученый секретарь научно-  
технической коллегии  
НП «НТС ЕЭС», к.т.н.

  
Я.Ш. Исамухамедов

Председатель секции  
«Автоматизированный учет  
электроэнергии и управление  
электропотреблением»,  
НП «НТС ЕЭС», к.т.н.

  
А.В. Покатилов

Ученый секретарь секции  
«Автоматизированный учет  
электроэнергии и управление  
электропотреблением»,  
НП «НТС ЕЭС»

  
Е.Ю. Евенок

**Список участников заседания секции «Автоматизированный учет электроэнергии и управление электропотреблением» НТС ЕЭС, состоявшегося 26 марта 2024 года**

1. Бартош Регина Тадэушевна, ПАО «Мосэнерго», приглашенный.
2. Большаков Олег Вадимович, Электроэнергетический Совет СНГ, член секции.
3. Бойченко Светлана Игоревна, Ассоциация «НП Совет рынка», приглашенный.
4. Быков Дмитрий Сергеевич, ПАО «Мосэнерго», член секции.
5. Васенков Алексей Евгеньевич, ПАО «Мосэнерго», приглашенный.
6. Воротницкий Валерий Эдуардович, АО «НТЦ ФСК ЕЭС», член секции.
7. Генгринович Евгений Леонидович, АО «ИнфоТеКС», член секции.
8. Громочкова Елена Витальевна, ФГБУ «ВНИИМС», приглашенный.
9. Губа Ирина Сергеевна, ПАО «Мосэнерго», член секции.
10. Дубровская Татьяна Анатольевна, ФГБУ «ВНИИМС», приглашенный.
11. Евенок Екатерина Юрьевна, ПАО «Мосэнерго», ученый секретарь секции.
12. Каспарова Екатерина Бююкагановна, ПАО «Мосэнерго», приглашенный.
13. Киселев Виктор Вячеславович, ФГБУ «ВНИИМС», член секции.
14. Коровкин Роман Владимирович, ФБУ «Ростест-Москва», член секции.
15. Кустиков Алексей Валерьевич, ООО НПП «ЭКРА», приглашенный.
16. Матисон Владимир Арнольдович, ООО НПП «ЭКРА», приглашенный.
17. Муртазалиева Фариза Хабибовна, ПАО «Мосэнерго», член секции.
18. Новиков Вадим Владимирович, член секции.
19. Покатилов Александр Васильевич, ПАО «Мосэнерго», руководитель секции.
20. Тацин Антон Вячеславович, ООО «Ситиэнерго», член секции.
21. Тимошенко Ольга Андреевна, ПАО «Мосэнерго», член секции.
22. Хавроничев Олег Валерьевич, ПАО «ТГК-1», член секции.
23. Чернецов Виктор Федорович, ФГБУ «ВНИИМС», член секции.
24. Шаталов Андрей Валерьевич, ПАО «Мосэнерго», приглашенный.