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, http://www.nts-ees.ru/
ИНН 7717150757

«УТВЕРЖДАЮ»

Председатель научно-технической коллегии НП «НТС ЕЭС»,
д.т.н. профессор
_____ Н.Д. Рогалев
«03» ноября 2022 г.

ПРОТОКОЛ

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

по теме

Факторы, влияющие на функциональную надежность (живучесть) цифровых систем

19.10.2022 г. № 19 г. Москва

Заседание проводилось в комбинированном формате (очно и дистанционно).

Присутствовали: 19 человек (список прилагается)

На заседании выступили:

С вступительным словом о работе секции выступил Александр Васильевич Покатилов - Председатель секции «Автоматизированный учет электроэнергии и управление электропотреблением». В его выступлении было отмечено, что в представленном, на рассмотрение членов секции и приглашенных, докладе предлагается рассмотреть новый подход к обеспечению живучести цифровых систем в электроэнергетике, в том числе в условиях неблагоприятных информационных воздействий. В определенной части доклад развивает темы, которые были затронуты на предыдущем заседании секции в докладе посвященном метрологии цифровых систем.

Доклад «Факторы, влияющие на функциональную надежность (живучесть) цифровых систем» (Приложение 1) представил Генгринович Евгений Леонидович, Советник Генерального директора АО «ИнфоТеКС».

Актуальность темы обусловлена фундаментальной цифровой трансформацией всех отраслевых бизнес процессов в рамках энергетической стратегии Российской Федерации на период до 2035 года. Стратегия предполагает структурную перестройку отрасли, в рамках

которой углеродная энергетика дополняется ВИЭ, развивается инфраструктура электрических транспортных средств, а параллельно обеспечивается процесс импортозамещения, направленный на приоритетное использование российских технологий. Цифровая трансформация бизнес-процессов сопровождается внедрением сервисно-ориентированных платформенных решений, обеспечивающих повышение производственной безопасности и эффективности эксплуатации энергетической инфраструктуры.

Важно отметить, что вопросы функциональной надежности (живучести) цифровых систем, где более 80% составляют ИТ-решения, требуют более детального рассмотрения. При сроке эксплуатации энергообъектов 20-25 лет, предугадать в каком объеме будут происходить нарушения нормального функционирования цифровых систем, маловероятно. Поэтому гораздо эффективнее действовать по аналогии с алгоритмами защиты от классических неблагоприятных внешних воздействий. К классическим неблагоприятным внешним условиям эксплуатации (НВУ) таким как природные катаклизмы, ошибки персонала, производственный брак, физические отказы при несоблюдении условий эксплуатации, добавились ошибки программного обеспечения (ПО), ошибки персонала при его конфигурировании, отказы сети передачи данных, несанкционированное вмешательство в процесс эксплуатации ПО и т.п. И если с классическими НВУ работают, путем различного рода аттестаций оборудования и персонала, а также повышением уровня дисциплины эксплуатации, то опасность новых типов НВУ, пока еще даже не полностью осознается, уже не говоря о том, чтобы обеспечивать меры по их предотвращению.

Решением для информационных НВУ могут стать специализированные встраиваемые решения, позволяющие обеспечить реализацию доверенных алгоритмов контроля корректности работы в нормальном режиме функционирования цифровых систем. Использование данных алгоритмов будет обеспечивать нейтрализацию НВУ с информационной составляющей, сохраняя при этом возможность обеспечения основных бизнес-услуг. На их базе будет формироваться, так называемая, киберустойчивость цифровых решений. Относительно новый термин «Киберустойчивость» можно определить, как способность предвидеть, противостоять, восстанавливаться и адаптироваться к неблагоприятным условиям, стрессам, компьютерным ошибкам или компрометации систем, включающих информационные ресурсы.

Анализ потенциально возможных информационных НВУ с разработкой штатных алгоритмов реагирования на них должен охватывать весь жизненный цикл продуктов и систем от проектирования изделия/системы до завершения срока эксплуатации цифрового решения, в составе которого, это изделие/система применяется. В международной практике

для этого процесса используется термин Security-by-design. Этот термин подразумевает вовлеченность непосредственно разработчика и проектировщика цифровых решений. С учетом особенностей требований к использованию средств криптографической защиты информации (далее – СКЗИ) в РФ, задачей компаний-разработчиков СКЗИ, становится предоставление необходимого сертифицированного инструментария, для решения поставленных задач.

Задача обеспечения живучести цифровых систем многослойна. Один из уровней - защищённая виртуальная телеком инфраструктура, обеспечит защиту коммуникационной составляющей цифровой экосистемы. Флагманской разработкой компании «ИнфоТеКС» является платформа ViPNet – гибкое решение для построения виртуальной защищенной сети для территориально распределенных объектов. Сегодня ViPNet – это самая масштабируемая и надежная платформа на российском рынке информационной безопасности. Есть опыт создания собственной инфраструктуры в виде NVF функций, а также интеграции с Амазон, Azure, Yandex etc. Опыт интеграции с первичными устройствами, в том числе, Siemens, Wago, Phoenix Contact, в стандартных Docker контейнерах и с рядом российских производителей ПЛК, непосредственно в Линукс окружение ПЛК.

Во встраиваемых СКЗИ представлено сертифицированное решение ViPNet SIES, для использования в качестве инструмента обеспечения живучести. SIES предназначен для встраивания в компоненты автоматизированных систем управления (АСУ), АСУТП, промышленного интернета вещей и систем межмашинного взаимодействия (M2M). В SIES реализован криптографический протокол, который соответствует нормативному документу Р 1323565.1.029 2019, что обеспечивает открытость решения, в которое могут быть интегрированы СКЗИ любых производителей, поддерживающие данный стандартизованный криптографический протокол. Решение трехуровневое, на нижнем уровне – это сертифицированные ПАК для встраивания в функциональное оборудование. Их использование позволяет предоставить разработчику набор стандартных криптографических функций для противодействия информационным НВУ. Решение полностью пассивно и не влияет на работу основного функционала. Крипточип позволяет обеспечить поддержку возможностей применения СКЗИ уже на уровне датчиков.

Наглядный пример, когда отраслевые требования оказывают влияние на регулирование в смежных отраслях. Так было с межповерочным интервалом измерительных трансформаторов тока и напряжения при запуске оптового рынка электроэнергии, теперь аналогичный процесс происходит в части изменения допустимого

срока хранения криптографических ключей на крипточипе. Для справки, классические требования к СКЗИ предполагают ежегодную замену ключей на конечном устройстве.

ViPNet SIES Core Nano – это полностью российская разработка, которая позволяет значительно упростить эксплуатацию территориально распределенных систем, за счет прошивки ключевой информации в крипточип на весь срок службы изделия. Сейчас идет процесс сертификации.

Если рассматривать ИСУЭ, как один из вариантов системы промышленного интернета вещей, то применение SIES также позволит существенно повысить эксплуатационную надежность создаваемой системы. Низкая стоимость крипточипа и возможность хранения ключей до 16 лет, обеспечивает эффективность его интеграции с приборами учета для ИСУЭ. Интеграция и загрузка ключей в крипточип будет происходить уже на этапе производства приборов учета, тем самым снимая эти вопросы с Заказчиков. На этапе опытно-промышленной эксплуатации ИСУЭ предусмотрен процесс инициализации ключевой системы уже всего решения в целом с привязкой к конкретному объекту эксплуатации.

Так как процесс интеграции СКЗИ SIES в компоненты цифровых экосистем требует временных и ресурсных затрат от производителей таких компонентов, необходимо организовать формирование отраслевой нормативной основы для обеспечения живучести цифровых экосистем, основанной на анализе рисков снижения функциональной надежности, на всех этапах жизненного цикла их компонент.

Будущее цифровой трансформации в электроэнергетике зависит от того, насколько быстро и эффективно удастся решить вопросы функциональной надежности и безопасности, внедряемых решений. Это напрямую будет влиять на достижение, заявленных показатели экономической эффективности цифровой трансформации в отрасли.

В обсуждении доклада приняли участие:

Представители АО «ИнфоТеКС», АО «НТЦ ФСК ЕЭС», ФГБУ «ВНИИМС», Ассоциация «НП Совет рынка», ФГБУ «Российское энергетическое агентство» Минэнерго России. Были подняты и обсуждались следующие вопросы.

Обозначили целесообразность дифференцировать определения таких терминов как функциональная надежность, безопасность, живучесть. Обратили внимание на необходимость пересмотра подхода оценки надежности цифровых решений с учетом роста информационной составляющей применяемых решений. Отметили тот факт, что для обеспечения функциональной надежности и информационной безопасности могут быть использованы одни и те же инструменты, что обеспечит синергетический эффект.

Рекомендовали, по возможности перейти на использование российских аббревиатур/терминов вместо иностранных, в рамках развития процессов по импортозамещению, во вновь создаваемых продуктах, а также необходимости конкретизации ранее заимствованных иностранных терминов с целью единого понимая их значения.

С помощью предложенных механизмов, можно обеспечивать защиту информации, регулировать локальный физический доступ к компонентам цифровых решений, проверять корректность конфигурации (что она получена именно из нужного источника и соответствует требованиям), проверять корректность применяемых расчетных алгоритмов. Например, совместно с НИУ МЭИ есть наработки для нового поколения терминалов релейной защиты.

В части опыта внедрения SIES в ИСУЭ отметили интеграцию с рядом производителей контроллеров (ИВКЭ). Российская компания «Завод Нартис» (дочерняя компания «Интер РАО») планирует выпуск контроллеров и счётчиков электроэнергии под проекты ИСУЭ, проведено встраивание, совместно согласовано с Регулятором техническое задание по встраиванию СКЗИ в контроллер, идут испытания в сертификационной лаборатории. Есть стенды с компанией «Системы и технологии» (г. Владимир), идут работы с рядом производителей счетчиков электроэнергии.

По информации полученной в ФГБУ «ВНИИМС» в рамках выполнения поручения Постановления Правительства РФ от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)» Минэнерго, Минцифра и ФСБ провели соответствующий анализ по поиску решений криптографической защиты информации ИСУЭ. Заключение показало, что производители не готовы дать решение по системе криптографической защиты информации для ИСУЭ. По информации ФСБ России, до настоящего времени материалы по тематическим исследованиям от специализированных организаций, производителей СКЗИ для УСПД и производителей УСПД на экспертизу в ФСБ России не поступили. Таким образом, сроки запуска производства УСПД с использованием сертифицированных СКЗИ до настоящего времени не определены. Базовая модель угроз безопасности информации подлежит пересмотру в срок до 31 декабря 2023 г. в части использования в приборах учета электрической энергии СКЗИ, сертифицированных ФСБ России.

Готовые встраиваемые СКЗИ не достаточное условие для того, чтобы стать частью системы. Для их внедрения необходимо время, подготовка людей, а потом и изделий. Есть разные подходы по внедрению СКЗИ, в связи с чем на уровень производителей (ИВКЭ,

прибуры учета электроэнергии) поступает противоречивая информация по требованиям к системе и ее компонентам, что усложняет работу и сроки реализации решений.

Одна из основных целей доклада - обратить внимание на необходимость разработки отраслевой нормативной документации, без которой невозможно развитие озвученных в докладе решений.

В целях повышения общего уровня надежности и безопасности предложили классические рекомендации для повышения функциональной надежности (живучести) цифровых систем:

- Архитектура систем должна иметь возможность деление ее на "отсеки", которые естественным образом изолируют ее от распространения аварии или действия кибератаки по всей структуре.
- В зависимости от важности решаемых Системой задач, ее окружения и оперативной обстановке на объектах, следует иметь горячий, теплый или холодный резерв цифровых модулей. Они будут подхватывать оборудование, выходящее из строя или выводимое из эксплуатации, для сохранения целостности системы.
- Периодическое архивирование уникальной и критической информации в системе на отдельные носители, которые изолированы от интернета и интранета с целью уменьшения вероятности воздействия на их результатах кибератак.
- Создание физических межсетевых экранов вокруг важных серверов системы.

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

- ✓ Не смотря на четкую грань между информационной безопасностью и надежностью работоспособности цифровой системы, для их обеспечения может использоваться одни и те же инструменты (СКЗИ).
- ✓ Важность и актуальность рассматриваемых в докладе вопросов.
- ✓ Заседание освещено в журнале журнал «Электроэнергия. Передача и распределение»: https://eepir.ru/new/vstraivaemye-algoritmy-kak-zalog-ustojchivosti-cifrovyh-sistem/.

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

1. Разослать утвержденный Протокол заседания секции в:
    - Минэнерго РФ (Заместителю Министра П.Н. Сниккарсу);
    - Минпромторг РФ (Заместителю Министра В.В. Шпаку);

- Минцифры РФ (Заместителю Министра А.М. Шойтову);
- Ростехнадзор РФ (Руководителю А.В. Трембицкому);
- АО «СО ЕЭС» (Председателю Правления Ф.Ю. Опадчему)

и просить в целях достижения, заявленных показателей эффективности и безопасности цифровой трансформации и импортозамещения в электроэнергетике:

1.1. организовать работы по рассмотрению предложений обеспечивающих надежность цифровых решений при работе в условиях неблагоприятных внешних информационных воздействий, учитывая, что эти предложения также приведут к сокращению затрат на обеспечение безопасности критической информационной инфраструктуры при внедрении цифровых систем и импортозамещении, т.е. являются экономически выгодными;

1.2. для формирования необходимого кадрового потенциала и повышения качества предупреждения и расследования причин аварий в электроэнергетики предусмотреть:

1.2.1. подготовку и внесение изменений в Постановление Правительства РФ № 846 от 28.10.2009 «Об утверждении Правил расследования причин аварий в электроэнергетике» в части касающихся исследования влияния неблагоприятных внешних информационных воздействий на процесс, в результате которого произошла авария или была создана аварийная ситуация, с назначением в комиссии по расследованию аварий, специалистов, имеющих необходимую квалификацию;

1.2.2. создать межведомственную рабочую группу по формированию требований к цифровым решениям, их компонентам и компетенциям специалистов, необходимых в процессах проектирования, производства, запуска в эксплуатацию, обслуживания и модернизации до момента полного списания и утилизации со всеми накопленными данными, а также требований к компьютерному моделированию цифровых систем и их информационного окружения с проведением виртуальных испытаний в критических сценариях, предусматривающих комбинации информационных, техногенных и природных воздействий.

2. Направить утвержденный Протокол заседания секции в Рабочую группу «Метрологическое обеспечение цифровых подстанций» при Федеральном агентстве по техническому регулированию и метрологии (Росстандарт) с просьбой

рассмотреть необходимость применения встраиваемых сертифицированных средств криптографической защиты в целях:

- контроля аутентичности информационных алгоритмов, используемых для формирования измерительных величин;
- цифрового контроля доступа к средствам измерений;
- легитимизации цифровых измерений в спорных ситуациях.

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

_____ **В. В. Молодюк**

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

_____ **А.В. Покатилов**

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

_____ **Я.Ш. Исамухамедов**

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 19 октября 2022 года

1. Алхонин Иван Геннадьевич, АО «ИнфоТеКС», приглашенный.
2. Большаков Олег Вадимович, Электроэнергетический Совет СНГ, член секции.
3. Виноградский Роман Вячеславович, АО «Мосэнергосбыт», приглашенный.
4. Воротницкий Валерий Эдуардович, АО «НТЦ ФСК ЕЭС», член секции.
5. Генгринович Евгений Леонидович, АО «ИнфоТеКС», член секции.
6. Григорьев Андрей Олегович, АО «ИнфоТеКС», приглашенный.
7. Гусева Екатерина, журнал «Электроэнергия. Передача и распределение» приглашенный.
8. Евенок Екатерина Юрьевна, ПАО «Мосэнерго», ученый секретарь секции.
9. Ежов Александр Николаевич, ФГБУ «Российское энергетическое агентство» Минэнерго России, приглашенный.
10. Иванов Андрей Игоревич, АО «ИнфоТеКС», приглашенный.
11. Иванов Иван Петрович, ООО «Транснефтьэнерго», член секции.
12. Кишкурно Эдуард Антонович, Ассоциация «НП Совет рынка», член секции.
13. Красильников Ярослав Сергеевич, АО «ИнфоТеКС», приглашенный.
14. Осика Лев Константинович, НИУ МЭИ, член секции.
15. Плакидин Роман Сергеевич, ООО «ИЦ «Энергосервис», приглашенный.
16. Покатилов Александр Васильевич, ПАО «Мосэнерго», руководитель секции.
17. Тащин Антон Вячеславович, ООО «Ситиэнерго», член секции.
18. Чернецов Виктор Федорович, ФГБУ «ВНИИМС», член секции.
19. Щитников Александр Яковлевич, член секции.