Некоммерческое партнерство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»

111 250, Москва, проезд Завода Серп и Молот,
дом 10, офис 608, Тел. (495) +7 495 012 60 07
E-mail: dtv@nts-ees.ru, http://www.nts-ees.ru/
ИНН 7717150757

Основана в 1724 году

Российская Академия Наук
Секция по проблемам НТП в энергетике
Научного совета РАН по
системным исследованиям в энергетике

УТВЕРЖДАЮ
Президент, Председатель
Научно-технической коллегии,
д.т.н., профессор

_____ Н.Д. Рогалев

«07» апреля 2025 г.

ПРОТОКОЛ № 5

совместного заседания Секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы» НП «НТС ЕЭС» и Секции по проблемам НТП в энергетике Научного совета РАН по системным исследованиям в энергетике

19 марта 2025 года г. Москва

Присутствовали: члены секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы» НП «НТС ЕЭС», представители ФГБОУ ВО «НИУ МЭИ», ФГБУН «ИНЭИ РАН», ФГБУН «ИСЭМ СО РАН», АО «Россети Научно-технический центр», Комитет ВИЭ РосСНИО, ГБОУ ВО «Нижегородский государственный инженерно-экономический университет», ФГБОУ ВО «Нижегородский ГТУ им. Р.Е. Алексеева», ФГБОУ ВО «Новосибирский государственный технический университет», ФГАОУ ВО «Уральский федеральный университет им. Б.Н. Ельцина», ФГБОУ ВО «Сибирский федеральный университет», ФГАОУ ВО «Национальный исследовательский Томский политехнический университет», ФГБОУ ВО «Казанский государственный энергетический университет», ООО НПП «Экра», ООО «РТСофт-СГ», всего **54** человек.

Со вступительным словом выступил председатель секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы», руководитель Центра интеллектуальных электроэнергетических систем и распределенной энергетики ФГБУН «Институт энергетических исследований РАН», д.т.н. Илюшин П.В.

Во вступительном слове было отмечено, что в настоящее время вопросы обеспечения информационной безопасности цифровых систем становятся все более актуальными. В России на текущий момент действует целый ряд нормативно-правовых актов в области обеспечения информационной безопасности, анализ содержательной части которых будет представлен в сегодняшнем докладе. Важно объективно рассмотреть, каким образом изложенные требования исполняются в субъектах электроэнергетики. Кроме того, на заседании необходимо рассмотреть современные научные подходы к выявлению кибератак, с использованием определенных математических методов и алгоритмов. В настоящее время самые сложные кибератаки на объекты электроэнергетики связаны с подменой информации, которую сложно распознать, так как необходимо не только обнаружить факт кибератаки, но и восстановить информацию посредством определенных алгоритмов, через смежные измерения. Это крайне важно, так как в результате подмены информации в системах защиты и автоматического управления, в том числе противоаварийного, возможно добиться их неправильного реагирования на схемно-режимную обстановку. Выявление подмены информации, вследствие такого несанкционированного вмешательства, является крайне актуальным, так как неправильное действие систем защиты и автоматического управления может привести к значительные последствия как для объектов электроэнергетики, так и для потребителей электроэнергии.

С докладом **«Обеспечение информационной безопасности в электроэнергетических системах с цифровыми электронными устройствами, системами защиты, автоматики и управления»** выступила Гурина Людмила Александровна, к.т.н., доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Отдела электроэнергетических систем ФГБУН «Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук» (г. Иркутск). Содокладчик – Куликов Александр Леонидович, д.т.н., профессор, профессор кафедры «Электроэнергетика, электроснабжение и силовая электроника» ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева» (г. Нижний Новгород).

Основные положения доклада приведены ниже. Презентация доклада прикладывается **(Приложение 1)**.

1. Представлен анализ нормативной базы в области информационной безопасности и доверенных программно-аппаратных комплексов.

Основными структурными элементами информационной безопасности информационных систем являются:

- цели защиты информации;
- субъекты, участвующие в процессах информационного обмена;
- угрозы безопасности информационных систем;
- уровни уязвимости информации и информационной инфраструктуры.

Обеспечение информационной безопасности состоит в достижении трех взаимосвязанных целей – целостности, доступности и конфиденциальности. Для защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего в себя комплекс взаимосвязанных мер с использованием специальных аппаратно-программных средств, организационных мероприятий, нормативно-правовых актов.

2. Согласно 187-ФЗ к субъектам критической информационной инфраструктуры (КИИ) относятся «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (объекты), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, обеспечивающие взаимодействие этих систем или сетей».

С 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), не могут осуществлять закупки (по 223-ФЗ) без согласования с федеральным органом исполнительной власти, уполномоченным Правительством РФ:

- иностранного программного обеспечения (ПО), в том числе в составе программно-аппаратных комплексов (ПАК), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры (ЗОКИИ);
- услуг, необходимых для использования этого ПО на принадлежащих им ЗОКИИ.

С 1 января 2025 г. органам государственной власти, заказчикам запрещается использование иностранного ПО на принадлежащих им ЗОКИИ. В 6-месячный срок необходимо реализовать комплекс мероприятий, направленных

на обеспечение преимущественного применения субъектами КИИ отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им ЗОКИИ, в том числе:

– определить сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им ЗОКИИ;

– обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных ПАК для КИИ.

С 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств.

3. Программно-аппаратный комплекс – это комплекс технических и программных средств (программного обеспечения), работающих совместно для выполнения одной или нескольких специальных задач, являющийся электронной вычислительной машиной или специализированным электронным устройством (устройствами), функционально-технические характеристики которого(-ых) определяются исключительно совокупностью программного обеспечения и технических средств, и не могут быть реализованы при их разделении. ПАК является самостоятельно используемым, законченным техническим изделием, имеющим серийный номер.

С вводом данного юридически значимого определения термин программно- аппаратный комплекс (ПАК), введенный Указом Президента РФ № 166, получил однозначное толкование, а его «ДОВЕРЕННОСТЬ» определяется Приказом ФСТЭК № 76 от 02.06.2020 г.

Переход субъектов КИИ Российской Федерации на преимущественное применение доверенных ПАК на принадлежащих им ЗОКИИ осуществляется до 1 января 2030 г. Не допускается с 1 сентября 2024 г. использование субъектами КИИ Российской Федерации на принадлежащих им ЗОКИИ ПАК, не являющихся доверенными программно-аппаратными комплексами, за исключением случаев отсутствия произведенных в Российской Федерации доверенных ПАК, являющихся аналогами приобретенных субъектами КИИ РФ ПАК. Доля доверенных ПАК на ЗОКИИ по состоянию на 31 декабря 2029 г. должна составлять 100 процентов в общем количестве ПАК на ЗОКИИ.

4. Типовыми отраслевые объектами КИИ для деятельности «Передача электроэнергии и технологическое присоединение к распределительным электросетям» и деятельности по распределению энергии являются:

– системы, предназначенные для управления, релейной защиты и автоматики, противоаварийной автоматики (системы РЗА подстанции);

– системы, предназначенные для управления технологическими процессами подстанции;

– интеллектуальные системы учета электроэнергии (ИСУЭ);

– системы, предназначенные для управления сбором и передачей информации подстанций;

– системы диспетчерского и технологического управления электрическими сетями и др.

5. Согласно рейтингу в 2024 г. Российская Федерация утратила свои прежние позиции, переместившись из группы стран с высоким уровнем кибербезопасности во вторую категорию из пяти возможных. Необходима подготовка новых специалистов и повышение квалификации имеющихся работников в этой области с учетом специфики электроэнергетической отрасли.

6. Представлены предложения по обеспечению кибербезопасности цифровых устройств и систем на примере системы SCADA, системы мониторинга переходных режимов (СМПР), а также АСУ ТП с аппаратной частью в виде контроллеров. Принципы анализа этих цифровых систем, предложенные подходы и методы обеспечения кибербезопасности также могут быть использованы и для цифровых систем управления, защиты и автоматики с учетом специфики этих объектов.

Системы SCADA и СМПР являются наиболее уязвимыми к кибератакам в информационных системах, поскольку система управления влияет на всю электроэнергетическую систему (ЭЭС) через управляющие воздействия или свои выходные данные. Последствия, вызванные реализованными кибератаками на эти системы, представляют наибольшую опасность для функционирования ЭЭС.

Надежное функционирование ЭЭС зависит от применяемых информационных и коммуникационных технологий в цифровых системах управления. В условиях цифровизации ЭЭС становится более уязвимой к информационным сбоям и кибер-инцидентам в информационных системах.

Кибератаки на систему SCADA и СМПР могут привести к выработке и реализации неправильных управляющих воздействий и к развитию аварийных ситуаций в ЭЭС.

7. Для предотвращения нарушения управления ЭЭС в условиях кибератак необходима разработка мер (способов, средств, методов) по обеспечению сохранения свойств кибербезопасности. Для решения этой задачи требуется

анализ и оценка влияющих факторов на системы управления, где важным инструментом являются методы теории рисков.

Риск представляет собой комбинацию вероятности реализации угрозы и последствий (ущерба) от нее в отношении защищаемого актива (ресурса). Последствия определяются уровнем воздействия.

Разработан подход к оценке риска кибербезопасности при управлении ЭЭС на основе информационных факторов, состоящий из двух этапов:

– оценка риска кибербезопасности при каждой реализованной киберугрозе;

– определение результирующей оценки риска.

В отсутствие нормативной базы в этом вопросе была разработана методика оценки рисков кибербезопасности, которая позволяет определить наиболее уязвимые цифровые объекты ЭЭС, уровень их защищенности, оценить последствия реализованных кибератак на цифровые объекты ЭЭС.

8. В отсутствие принятой нормативной базы, предложенная методика оценки рисков кибербезопасности позволяет определить наиболее уязвимые цифровые объекты ЭЭС, уровень их защищенности, оценить последствия реализованных кибератак на цифровые объекты ЭЭС.

9. Представлены методы достоверизации данных измерений, используемых при управлении ЭЭС, а также решение задачи оценивания состояния при различных кибератаках на систему SCADA и СМПР.

Надежное функционирование ЭЭС может быть нарушено из-за неполноты и недостоверности измерений SCADA и СМПР.

Разработан алгоритм достоверизации данных на основе вейвлет-анализа. Достоинством применения вейвлет-преобразований потоков измерений является снижение влияния кибератак на достоверность информации путем фильтрации шумов и удаления (сглаживания) ошибок в измерениях.

10. Предложен алгоритм обнаружения ошибочных измерений, возникающих при кибератаках и не идентифицируемых традиционными методами достоверизации измерений при оценивании состояния ЭЭС.

11. Разработан подход к оцениванию состояния ЭЭС на основе метода внутренней точки, позволяющий в случае потери измерений получить их оценки. Результаты расчетов показали эффективность использования предложенного подхода решения задачи оценивания состояния ЭЭС при кибератаке.

12. Для сохранения функциональности цифрового объекта при кибератаке на информационные системы ЭЭС необходимо обеспечение более быстрых отклика и восстановления аппаратных средств, программного обеспечения и взаимодействия цифровых объектов информационной системы, которые могут

быть охарактеризованы наименьшей интенсивностью отказов и максимальной интенсивностью восстановлений.

13. Уровень устойчивости цифрового объекта информационной системы при кибератаках можно охарактеризовать:

– приемлемым уровнем кибербезопасности;

– вероятностью безотказной работы;

– вероятностью восстановления составляющих цифрового объекта.

С учетом этого разработана иерархическая система определения показателя устойчивости информационной системы ЭЭС при кибератаках.

14. Отличительной особенностью предложенной методики является комплексный подход, позволяющий при определении показателя устойчивости учитывать оценку риска кибербезопасности, влияние качества информации и такие показатели надежности, как интенсивности отказов и восстановлений цифровых объектов информационной системы при кибератаках.

Анализ состояний таких цифровых объектов, как системы управления, системы противоаварийного управления, системы сбора, обработки и передачи информации на основе предложенной методики позволит реализовать мероприятия по повышению их защищенности и более обеспечить быстрое восстановление при кибератаках на ЗОКИИ в ЭЭС.

15. Разработан метод обнаружения и подавления последствий кибератак на взаимосвязанные информационные системы микросетей, состоящий из следующих этапов:

– моделирование взаимосвязанных микросетей;

– моделирование кибератак, оценка распространения их влияния на взаимосвязанные информационные системы микросетей;

– разработка возможных мер, обеспечивающих защищенность информационные системы микросетей от кибератак.

16. Использование предлагаемого подхода позволит своевременно обнаруживать место локализации кибератаки, не допускать распространение кибератаки на соседние контроллеры и восстанавливать качество данных, используемых при вторичном регулировании напряжения.

17. Важным и актуальным направлением является решение вопросов обеспечения информационной безопасности (кибербезопасности) цифровых объектов ЭЭС. Направление характеризуется быстро и динамично развивающейся нормативной базой в области информационной безопасности.

18. В существующей отраслевой практике, к сожалению, недостаточно нормативных документов, содержащих методические рекомендации по обеспечению кибербезопасности ЭЭС с конкретно применяемыми цифровыми устройствами, системами защиты, автоматики и управления.

19. Жесткие сроки по реализации планов перехода на доверенные ПАК и решение вопросов кибербезопасности, а также условия и переход противостояний из активной фазы боевых действий в киберсферу, стимулируют развитие новых исследований в области информационной безопасности (кибербезопасности) ЭЭС и разработку методов по ее обеспечению.

20. Целесообразно апробировать предложенные методики на цифровых энергообъектах, в том числе с распределенными энергетическими ресурсами.

21. Важна разработка методических рекомендаций по обеспечению кибербезопасности и связанных с ними других методик, направленных на оценку надежности, поскольку кибербезопасность является компонентом надежности.

22. Необходима разработка типовых доверенных ПАК и типовых решений на доверенных ПАК для цифровых объектов электроэнергетики, в том числе включающих распределенные энергетические ресурсы.

23. Необходима реализация отраслевых НИОКР в области обеспечения информационной безопасности энергообъектов с последующей апробацией методик по оценке киберзащищенности с учетом опыта эксплуатации.

24. Перспективным является исследование новых вероятностных моделей, которые будут положены в основу методики оценки уровней киберзащищенности и устойчивости цифровых систем ЗОКИИ и всей электроэнергетической системы в целом.

25. В настоящее время реализуется комплексная программа цифровизации электроэнергетики. На ПАО «Россети» возложена задача цифровизации в области передачи и обмена информации, что представляет реальный единственный путь, который может повысить эффективность и надежность функционирования ЭЭС. Следует отметить, что надежность цифровых систем во многом будет определять надежность ЭЭС в целом.

26. Большое количество опасностей с позиции кибербезопасности для информационных систем находится внутри субъектов электроэнергетики. Следовательно, разработка процедур обеспечения информационной безопасности и обеспечения доступа персонала к ЗОКИИ должно быть организовано на соответствующем уровне.

В обсуждении доклада и прениях выступили:

Илюшин П.В., Вольный В.С. (ФГБУН «ИНЭИ РАН»), Белоусов С.В. (ФГБОУ ВО «НИУ «МЭИ»»), Бык Ф.Л. (ФГБОУ ВО «НГТУ (НЭТИ)»), Воротницкий В.Э., Рабинович М.А. (АО «Россети Научно-технический центр»), Капустин А.В. (АО «СО ЕЭС»), Правиков Д.И. (Ассоциация «Цифровая энергетика»), Папков Б.В. (ФГБОУ ВО «НГИЭУ»).

Илюшин П.В. – Председатель секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы» НП «НТС ЕЭС», руководитель Центра интеллектуальных электроэнергетических систем и распределенной энергетики ФГБУН «ИНЭИ РАН», д.т.н.

Отметил, что во второй части доклада в приведенном примере определена не оценка риска, а средняя вероятность угрозы наступления какого-то события, поскольку не учитывался нанесенный экономический ущерб.

Попросил пояснить, что у нас все-таки не хватает специалистов в области информационной безопасности или не хватает специалистов соответствующей квалификации для развития и совершенствования системы обеспечения информационной безопасности в субъектах электроэнергетики.

Отметил, что необходимо выстраивание систему по двум направлениям. Первое связано с реализацией программ повышения квалификации для получения дополнительных знаний в области обеспечения информационной безопасности для специалистов, работающих в отрасли. Параллельно необходима подготовка энергетиков со знаниями в области информационной безопасности. Учитывая величину дефицита кадров в этой области, проблема с их подготовкой является крайне актуальной. Важно понимание, что курсами повышения квалификации на 30-50 часов задачу полноценно не решить. Нужна полноценная переподготовка (512 часов – это фактически годовой курс). Субъектам электроэнергетики нужно планировать эту деятельность.

Отметил, что вторая часть доклада ясно показано, что при подмене информации невозможно решить вопрос обеспечения информационной безопасности без понимания особенностей технологических вопросов. Требуется понимать, что происходит, как происходит, а также владеть математическим аппаратом оценивания состояния ЭЭС. Для решения задачи обеспечения информационной безопасности важно знание допустимых режимов ЭЭС.

Отметил, что коэффициент готовности оборудования в ЭЭС можно поддерживать на достаточном уровне за счет совершенствования системы обеспечения информационной безопасности, но если попытаться создать все системы в соответствие с жесткими требованиями по информационной безопасности, то это будет очень дорого и практически нереализуемо. Нужно определить разумный круг вопросов, объектов, где нужно этим вопросам уделить особое внимание и вкладывать значительные средства. Минимизация времени восстановления также влияет на величину коэффициента готовности. Нужны специальные бригады, осуществляющие восстановительные работы после кибератак. Необходимо создавать такие подразделения, которые будут оперативно выявлять, разбираться и устранять последствия, тем самым минимизируя время восстановления и повышая коэффициент готовности.

Обратил внимание на то, что микросети организуются в сетях, как правило, низкого напряжения, в некоторых случаях среднего напряжения. В микросетях ущербы небольшие и они не относятся к ЗОКИИ. Задал вопрос, почему именно микросети были выбраны в качестве объекта исследования в вопросах реализации мероприятий в области информационной безопасности?

Отметил зависимость технологической части ЭЭС от информационно-коммуникационной инфраструктуры. Существуют объекты энергетики, которые не пользуются собственными каналами связи. Сейчас требования к каналам связи и скорости передачи информации существенно возросли. При применения централизованных алгоритмов управления нужны высокоскоростные каналы связи с большой пропускной способностью, что вынуждает переходить на применение волоконно-оптических линии связи, при этом сетевые компании их не имеют. Они арендуют чужие каналы связи у различных операторов связи. Существует сильная зависимость от чужой инфраструктуры, которая не относится к собственности объектов электроэнергетики.

Задал вопрос, касающийся рассмотрения возможности применения, где это возможно, децентрализованных алгоритмов управления, которые не зависят от каналов связи и обладают существенными преимуществами в части информационной безопасности.

Отметил, что область обеспечения информационной безопасности в ЭЭС новая и достаточно сложная, поэтому без квалифицированных специалистов будет крайне сложно решить этот вопрос.

Отметил отраслевую специфику обеспечения информационной безопасности ЭЭС, которая связана с особенностями выявления подмены данных (допустимые параметры режима; восстановление данных по смежным измерениям), а также последовательностью восстановления ЭЭС после отключения отдельных объектов.

Белоусов С.В. – Проректор по цифровой трансформации ФГБОУ ВО «НИУ МЭИ», к.т.н., доцент.

Отметил, что в НИУ «МЭИ» имеется направление и кафедра по информационной безопасности, на которой ведется подготовка специалистов по информационной безопасности на протяжении уже нескольких лет. Поэтому говорить о том, что в энергетических ВУЗах специалистов по информационной безопасности не готовят не совсем корректно.

Бык Ф.Л. – Доцент кафедры Автоматизированных электроэнергетических систем ФГБОУ ВО «НГТУ (НЭТИ)», к.т.н., доцент.

Обратил внимание на то, что панацея борьбы с позиции кибербезопасности

– это уходить на децентрализованное управление, которое позволяет даже при единичных и даже двойных отказах не потерять всю систему.

Задал вопрос, почему к объектам КИИ не относятся АСКУЭ и системы управления реклоузерами? Отметил, что в этих системах передача информации осуществляется не по выделенным арендованным каналам связи, а по GPS-каналам. В этом случае хакером может выступать лицо или компания, заинтересованная в изменении данных АСКУЭ, что приведет к необходимости оплачивать большие суммы за электроэнергию со стороны потребителей.

Отметил, что в докладе рассмотрены технические аспекты и предложил включить в дальнейшие исследования экономические аспекты, например, оценку последствий от изменения информации, поступающей от АСКУЭ в расчетную систему платежей за электроэнергию.

Отметил, что управление реклоузерами через GPS-каналы связи позволяет изменять конфигурацию сети, что может крайне негативно повлиять на надежность электроснабжения потребителей, однако системы управления реклоузерами не относятся к ЗОКИИ.

Отметил, что помимо ЭЭС не менее серьезными системами, обеспечивающими жизнедеятельность, являются системы теплоснабжения, водоснабжения и водоотведения, которых нет ни в одном списке ЗОКИИ.

Отметил, что в докладе рассмотрены вопросы защиты информационных систем от внешних кибератак, а внутренние кибератаки со стороны отдельных субъектов электроэнергетики являются не менее опасными для потребителей.

Воротницкий В.Э. – Главный научный сотрудник АО «Россети Научно-технический центр», д.т.н., профессор.

Отметил, что когда говорится об обеспечении информационной безопасности цифровых системы, то нужно учитывать не только релейную защиту, оборудование регулирования напряжения, но и интеллектуальные цифровые системы учета электроэнергии. Они входят в перечень информационных источников и вопросы информационной безопасности систем учета электроэнергии в равной степени должны рассматриваться и разрабатываться. Если потеряется эта информация, то могут быть довольно большие составляющие ущерба, как экономические, так и технические.

Обратил внимание на то, что доклад касается достоверизации данных, оценивания состояния и это важно и нужно, но это только часть информационной безопасности. Информационная безопасность – это системное и комплексное понятие, поэтому задачи, которые были рассмотрены в докладе являются частью большой системы вопросов, подлежащих решению.

Отметил, что к подготовке специалистов в области информационной безопасности обязательно должны подключаться специалисты-энергетики. Нужна подготовка не только студентов, но и преподавателей по указанным вопросам, чтобы компенсировать большую нехватку персонала.

Рабинович М.А. – Главный научный сотрудник АО «Россети Научно-технический центр», д.т.н., старший научный сотрудник.

Задал вопрос, в чем основная идея использования вейвлет-анализа в задаче обеспечения информационной безопасности.

Капустин А.В. – Заместитель начальника службы – начальник отдела Службы информационной безопасности АО «СО ЕЭС».

Обратил внимание на то, что в докладе были освещены вопросы информационной безопасности, но хочется дополнить его информацией о взаимодействии субъектов электроэнергетики. Требуется реализация комплексного подхода с учетом отраслевой специфики.

Отметил, что достоверизация данных является одним из важных аспектов обеспечения информационной безопасности.

Обратил внимание на то, что в настоящее время Минэнерго России ведет активную работу в области обеспечения информационной безопасности, определены электросетевые объекты ПАО «Россети». Разработаны и другие нормативные документы, которые нужно учитывать в анализе. Для обмена опыта необходим обмен и ведение единой базы документации. По линии АО «СО ЕЭС» разрабатываются новые документы совместно с Минэнерго России.

Отметил недостаточное количество квалифицированных кадров в области информационной безопасности. Необходима разработка курсов переподготовки и повышения квалификации, где бы рассматривались актуальные вопросы обеспечения информационной безопасности в условиях современных угроз.

Правиков Д.И. – Представитель Ассоциации «Цифровая Энергетика».

Обратил внимание на то, что сейчас идет этап формирования подходов к обеспечению информационной безопасности с учетом отраслевой специфики. Большая часть организационно-технических мероприятий общего плана уже были реализованы в большинстве энергокомпаний.

Отметил, что доклад хороший и это шаг вперед в рассматриваемой области. В докладе выделены конфиденциальность, целостность и доступность. Приведено определение из ФЗ №187 о состоянии защищенности ЗОКИИ, обеспечивающей устойчивость функционирования.

Отметил, что помимо предложенной методики оценки рисков существуют и другие, учитывающие специфику кибератак на объекты электроэнергетики, и задал вопрос, было ли проведено их сравнение?

Задал вопрос, что такое информационная безопасность с отраслевой спецификой электроэнергетики?

Задал вопрос, возможны ли атаки захвата контроллеров при реализации нормативного документа № 239 ФСТЭК.

Папков Б.В. – Профессор кафедры «Электрификация и автоматизация» ФГБОУ ВО «Нижегородский государственный инженерно-экономический университет», д.т.н., профессор.

Обратил внимание на то, что если происходит кибератака на ЗОКИИ, то эта кибератака может быть успешной или неуспешной. При успешной реализации кибератаки, как и в надежности, происходит развитие отказа?

Задал вопрос, есть ли какие-то статистические данные или информация об условной вероятности кибератак на системы электроснабжения промышленных предприятий или других потребителей электроэнергии в России и мире? Отметил, что при отсутствии статистики, нельзя говорить об ущербах.

Задал вопрос о том, какой приемлемый уровень риска кибербезопасности?

Задал вопрос о том, рассматривалось ли применение игровых методов в области обеспечения информационной безопасности?

Вольный В.С. – Аспирант ФГБУН «Институт энергетических исследований Российской академии наук».

Задал вопрос о том, что такое кибератака на системы релейной защиты?

Отметил, что комплекс информационной безопасности, в том числе предотвращает возможность несанкционированного доступа в электроустановки и уже является одним из ключевых методов, который исключает кибератаки. В электроустановках есть возможности по непосредственному воздействую на электрооборудование в части изменения его коммутационного состояния.

Отметил, что коммутационными аппаратами невозможно управлять с помощью телеуправления, а только через SCADA-системы оперативно-технологическим персоналом.

Отметил, что все электрооборудование может находиться на местном управлении, что исключает возможность его дистанционного управления.

В настоящее время используются сплит-счетчики, т.е. один счетчик стоит в компании, который сигнал передает АСКУЭ, а второй – у потребителя.

Заслушав выступления экспертов по результатам дискуссии совместное заседание Секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы» НП «НТС ЕЭС» и Секции по проблемам НТП в энергетике Научного совета РАН по системным исследованиям в энергетике **отмечает:**

1. Учитывая, что разработанная методика оценки рисков кибербезопасности основана на вероятностных моделях угроз и нарушений, то ее применение целесообразно при разработке комплекса организационно-технических мероприятий по снижению влияния киберугроз на ЗОКИИ ЭЭС.
2. Разработанный метод обнаружения ошибочных измерений с подменой информации при кибератаках позволяет своевременно исключать влияние успешно реализованных кибератак на результаты оценивания состояния ЭЭС, тем самым обеспечивая реализацию корректного управления электрооборудованием на основе достоверной информации.
3. Разработанные методики и подходы могут найти свое применение при проектировании и эксплуатации систем защиты, автоматики и управления, где существует информационный обмен между цифровыми объектами.

Совместное заседание Секции «Активные системы распределения электроэнергии и распределенные энергетические ресурсы» НП «НТС ЕЭС» и Секции по проблемам НТП в энергетике Научного совета РАН по системным исследованиям в энергетике **решило:**

1. Рекомендовать автору учесть высказанные рекомендации в дальнейших научных исследованиях и разработках в области обеспечения кибербезопасности электроэнергетических систем.
2. Рекомендовать автору при разработке новых методов и алгоритмов учитывать, помимо внешних, внутренние угрозы с позиции кибербезопасности электроэнергетических систем.
3. Рекомендовать руководителям и специалистам в области информационной безопасности субъектов электроэнергетики ознакомится с разработанными методиками и подходами, а также рассмотреть возможность их применения в практической деятельности.
4. Рекомендовать ВУЗам и организациям дополнительного профессионального образования рассмотреть возможность разработки курсов переподготовки и повышения квалификации в области информационной безопасности, с учетом отраслевой специфики.

С заключительным словом выступил председатель секции «Активные системы распределения электроэнергии и распределенные энергетические

ресурсы» НП «НТС ЕЭС», д.т.н. Илюшин П.В., в котором отметил важность рассмотренной темы и наличие в ней специфики электроэнергетической отрасли. Переход на децентрализованную энергетику с децентрализованными системами управления, который реализуется в настоящее время, имеет все основания, но электроэнергетические системы должны надежно функционировать в условиях современных угроз в области информационной безопасности. Кроме того, часть алгоритмов противоаварийного управления, а также оптимизационные алгоритмы невозможно реализовать без передачи данных по каналам связи. В условиях возникновения новых угроз, необходимо разрабатывать современные методы, алгоритмы и модели, позволяющие адекватно на них реагировать. Для этого необходимо четко оценивать последствия тех или иных угроз от кибератак на ЗОКИИ ЭЭС. Сегодняшнее заседание является первым по данной тематике на нашей секции НП «НТС ЕЭС». Оно позволило поднять и обсудить основные вопросы в области информационной безопасности, а на часть вопросов получить ясные ответы. Авторы доклада представили промежуточные результаты в рассматриваемой области, но как было отмечено в докладе, разработки будут продолжены. Уверен, что экспертное сообщество по достоинству оценит полученные результаты, а высказанные рекомендации поспособствует развитию исследований с учетом специфики электроэнергетики при формировании подходов, принципов использования математических методов как для выявления кибератак, так и устранения их последствий.

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 «АСРЭ и РЭР»
НП «НТС ЕЭС», ученый секретарь
Секции по проблемам НТП в энергетике
Научного совета РАН по системным
исследованиям в энергетике, д.т.н.

_____ П.В. Илюшин

Ученый секретарь секции
«Активные системы распределения
электроэнергии и распределенные
энергетические ресурсы» НП «НТС
ЕЭС», к.т.н.

_____ Д.А. Ивановский