Некоммерческое партнерство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»

Российская Академия Наук
Секция по проблемам надёжности и
безопасности больших систем
энергетики Научного совета РАН по
системным исследованиям в энергетике

УТВЕРЖДАЮ
Президент НП «НТС ЕЭС»,
д.т.н., профессор

Н. Д. Рогалёв

ПРОТОКОЛ

совместного заседания Научно-технического совета НП «НТС ЕЭС»
и Секции по проблемам надёжности и безопасности больших систем энергетики
Научного совета РАН по системным исследованиям в энергетике на тему:
«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»

г. Москва № 2/20 16 декабря 2020 г.

Заседание проведено в режиме видеоконференции.

В видеоконференции приняли участие: АО «СО ЕЭС», Центр НТИ МЭИ, Лаборатория Касперского, Positive Technologies, ИСЭМ СО РАН, Отделение энергетики, машиностроения, механики и процессов управления РАН, Совет РАН по проблемам развития энергетики, АО «Техническая инспекция ЕЭС», научно-исследовательские и образовательные институты, организации энергетического профиля и др. Всего 92 участника.

Заседание открыл первый заместитель председателя Научно-технической коллегии НП «НТС ЕЭС» д.т.н., профессор **В. В. Молодюк**.

В своём вступительном слове В. В. Молодюк отметил важность проблемы кибербезопасности РЗА и систем управления современных объектов электроэнергетики. В виду важности проблемы заседание решено провести в расширенном формате дополнительным с участием следующих секций НП «НТС ЕЭС»:

- «Проблемы надёжности и эффективности релейной защиты и средств автоматического системного управления в ЕЭС России», председатель секции к.т.н. **А. В. Жуков**;

- «Управление режимами энергосистем, РЗА», председатель секции **А. Ф. Бондаренко**;
- «Надёжность энергетических систем и энергетическая безопасность», председатель секции член-корр. РАН **Н. И. Воропай**.

Подготовку заседания обеспечивала секция «Проблемы надёжности и эффективности релейной защиты и средств автоматического системного управления в ЕЭС России», председателем которой является к.т.н. **А. В. Жуков**.

Со вступительным словом выступил руководитель секции «Проблемы надежности и эффективности релейной защиты и средств автоматического системного управления в ЕЭС России», советник директора АО «СО ЕЭС», к.т.н. **А.В. Жуков**

С докладами выступили:

- «Возможные методы анализа последствий влияния кибератак на системы релейной защиты и автоматики цифровых и высокоавтоматизированных подстанций», **В. Г. Карантаев**, **В. И. Карпенко** (Центр НТИ МЭИ);
- «Кибербезопасность устройств Цифровой подстанции», **С. С. Корт, В. Г. Карантаев** (Лаборатория Касперского);
- «Центры кибербезопасности. Ситуационная осведомлённость и управление реагированием», **Д. Даренский** (Positive Technologies, групповой член СИГРЭ);
- «Предлагаемые методы и средства защиты объектов цифровой энергетики», к.т.н. **М. В. Никандров** — руководитель ПРГ № 2 РНК СИГРЭ D2/B5 «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»;
- «Разработка и внедрение комплексов РЗА ЦПС с различными архитектурами», **Н. Лебедева** (Центр НТИ МЭИ).

Совместное заседание отмечает

1. Проблематика вопроса

Ускоренное развитие информационно-коммуникационных технологий (ИКТ) в настоящее время является одной из наиболее характерных особенностей современного мира, основой процессов цифровой трансформации общества, базовой инновационной платформой развития и внедрения современных цифровых технологий во всех областях жизни человека, общества и государства (управление, бизнес, образование, медицина, энергетика, и промышленность). В то же время, именно благодаря своему глобальному проникновению во все аспекты жизни общества и государства, цифровые технологии могут стать угрозой стабильности развития и самого существования общества. Во всех странах мира активно обсуждается широкий спектр вопросов, связанных с проблемой обеспечения информационной безопасности технологических систем, мировыми киберугрозами, международной безопасности и стабильности.

На уровне международных организаций (таких как ООН, Советы по безопасности и т. д.) обсуждаются меры по обеспечению международной информационной безопасности и меры доверия, формальные обязательные соглашения по киберпространству, и технические, этические, а также

юридические вопросы использования ИКТ в гражданской и военной сфере, и предложения по запрету кибератак на критически важную государственную инфраструктуру.

Во многом это связано с лавинообразным ростом конкретных фактов применения вредоносных ИКТ в военных конфликтах, увеличением количества кибератак на критически важную государственную инфраструктуру с уже не гипотетической, а реальной возможностью применения военной силы даже не в ответ, а в целях предотвращения кибератаки с соответствующими изменениями, которые вносятся в стратегические документы все большего количества стран.

В качестве наиболее ярких примеров такого воздействия можно вспомнить использование компьютерных вредоносных программ Stuxnet, Duqu, Wiper, Flame, Industroyer, Triton, PoetRAT и др., применяемых для комплексных массированных кибератак на критически важные объекты государственной инфраструктуры различных отраслей и стран. Их направленность демонстрирует, что проблема кибербезопасности для критической информационной инфраструктуры действительно существует.

Одним из важнейших и критичных сфер многие государства признают сферы, связанные с энергетикой. Энергетическая инфраструктура стала основной целью кибератак за последнее десятилетие, причем все чаще совершаются изощренные атаки со стороны национальных государств и киберпреступников.

Повышение уровня автоматизации объектов электросетевого хозяйства средствами современных информационно-технологических и телекоммуникационных технологий, сооружение современных технологических объектов с развитой информационной инфраструктурой, переход от проприетарных низкоскоростных протоколов и интерфейсов (RS485, IEC60870-5-101, IEC60870-5-103, ModBus и т. д.) на современные высокоскоростные сети передачи данных (Ethernet, IEC61850) — все это значительно увеличило поверхность для компьютерных атак и возможность проникновения злоумышленников в контур технологического управления.

Так, например, во вредоносном программном обеспечении Industroyer были впервые использованы настройки под конкретные протоколы, используемые в электроэнергетике.

С усложнением векторов кибератак, используемых тактик атаки и непрерывно модернизируемых средств защиты злоумышленники сместили цель с простых блокировок данных или кражи информации на нарушение технологического процесса и причинение физического ущерба.

Сегодняшняя реальность показывает, что киберинцидент может нарушить технологический процесс, повредить узкоспециализированное оборудование и поставить под угрозу здоровье, безопасность и даже жизнь людей. Из вышесказанного можно сделать вывод, что вопросы, связанные с обеспечением информационной и кибербезопасности в сфере энергетики и топливно-энергетического комплекса (ТЭК), являются приоритетными направлениями развития национальной безопасности для многих государств. Перед возрастающей киберугрозой государства начали предпринимать попытки выработки национальных стратегий и стандартов по обеспечению информационной безопасности, в том числе специализированные для энергетики.

Тренд на цифровизацию и импортозамещение отрасли электроэнергетики ставит однозначный вопрос о необходимости обеспечения приемлемого уровня кибербезопасности и гармонизации процессов развития технологий управления и обеспечения надёжности функционирования современных цифровых комплексов автоматического управления, прежде всего, систем релейной защиты и автоматики (РЗА). Системы РЗА имеют крайне высокую степень критичности для обеспечения устойчивой и надёжной работы энергосистемы, при этом современные технические средства РЗА переведены на цифровую и IT платформы, что приводит к эскалации проблематики кибербезопасности.

2. Мировые тренды кибербезопасности

Стоит также отметить, что риски кибербезопасности становятся все более широко распространённым явлением, которые описываются в периодических отчетах исследовательских центров промышленной кибербезопасности (таких как Dragos, Kaspersky, Positive Technologies и многих других). Согласно отчётам, к основным рискам защищенности промышленных объектов (ICS) в 2020 году можно отнести:

- существенное возрастание реализации атак, направленных на нарушение работоспособности критической инфраструктуры;
- целенаправленный фишинг на промышленные объекты, расположенные внутри периметра локальных сетей компаний;
- значительное увеличение всех типов атак на RDP (Remote Desktop Protocol) (в том числе связанное с влиянием пандемии COVID-19);
- использование вредоносного программного обеспечения (ПО) вирусов-вымогателей;
- рост атак на цепочки поставок (внедрение вредоносного ПО в легитимный код разработчиков).

Угрозы становятся более локальными, более фокусированными, и, как следствие — более разнообразными и сложными.

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются корпоративные сети и сети общего пользования (интернет), съёмные носители и электронная почта.

3. Международный опыт в вопросах обеспечения кибербезопасности

Проблема обеспечения кибербезопасности имеет общемировой характер и признана всеми развитыми странами, о чём свидетельствуют множественные научные статьи, работы различных некоммерческих организаций, онлайн публикации и доклады экспертов по кибербезопасности на специализированных Международных Форумах (CIGRE session, Black Hat Conference, DEFCON, RSA Conference, SANS Series, InfoSecurity Europe и т. д.).

Вопросы обеспечения кибербезопасности регламентируются различными международными комитетами, такими как IEC, IEEE и CIGRE. Особенно стоит отметить стремительно развивающиеся международные стандарты серии IEC 62351 и IEC 62443.

Одним из основных наборов международных методических документов по обеспечению кибербезопасности промышленных систем автоматизации является семейство стандартов IEC 62443. Серия стандартов IEC 62443 основывается на

риск-ориентированном подходе: безопасность рассматривается как совокупность непрерывных процессов, которые необходимо поддерживать на всех стадиях жизненного цикла системы. В IEC 62443 сформированы требования как к проектированию наложенных систем управления кибербезопасностью, так и к проектированию автоматизированных систем промышленной автоматизации технологических процессов (АСУ ТП) с уже встроенными и интегрированными мерами безопасности.

Кроме того, серия стандартов IEC 62443 требует внедрения хорошо известных специалистам, знакомым с семейством ISO 27000, следующих процессов: управление инцидентами, управление изменениями, управление конфигурациями, планирование восстановления деятельности и непрерывности процесса, повышение осведомленности и т. д., с учётом специфики промышленных систем автоматизации, АСУ ТП и SCADA систем (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных). IEC 62443, как и все стандарты и лучшие практики в области ИБ, подразумевает поддержку непрерывного жизненного цикла процессов безопасности, включает в себя постоянный пересмотр уже обработанных рисков, идентификацию и анализ новых, анализ эффективности принятых компенсационных мер и изменяющегося пространства рисков и угроз и т. д. на всех стадиях существования объекта защиты (промышленных систем автоматизации, АСУ ТП и SCADA систем).

Помимо стандартов IEC 62443 существует серия стандартов IEC 62351, в которых описаны требования безопасности для передачи сообщений IEC 61850 в пределах подстанций.

Стандарты направлены на описание требований безопасности протоколов серии ТС 57 и включают аутентификацию передачи данных с помощью цифровых подписей, обеспечение аутентифицированного доступа, предотвращение перехвата, предотвращение воспроизведения и спуфинга и обнаружение вторжений и т. д.

Помимо активно развивающихся вышеуказанных серий стандартов существуют различные исследования и рекомендации для применения требований информационной безопасности в части РЗА и центров управления, которые прорабатываются международными группами СИГРЭ. Из уже завершивших свою работу исследований можно сказать о следующих технических брошюрах: WG B5.38 «The Impact of Implementing Cyber Security Requirements using IEC 61850» и WG B5.66 «Cybersecurity requirements for PACS and the resilience of PAC architectures».

Помимо указанных международных групп, завершивших свою работу, сейчас ведутся работы в области кибербезопасности электроэнергетики в международной рабочей группе WG D2.51 «Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System».

4. Развитие международной нормативной и технической базы в области промышленной кибербезопасности (ICS)

В настоящее время всё более широкое применение получают микропроцессорные устройства с большими вычислительными возможностями для задач управления и автоматизации в электроэнергетической промышленности, в том числе для задач РЗА, систем SCADA, дистанционного

управления и мониторинга, а также для многих других приложений. Однако кроме очевидных технологических и технических преимуществ, обеспечиваемых микропроцессорной техникой, существует проблема угрозы информационной безопасности, возрастающая по мере увеличения количества цифровых объектов электроэнергетики (для электроэнергетики наиболее значимыми являются такие объекты как цифровые подстанции (ЦПС) с возможностью доступа по IP, обусловленная возможными несанкционированными действиями и рядом других рисков кибербезопасности.

До настоящего времени проектирование систем защиты и автоматизации объектов электроэнергетики осуществлялось в предположении на относительную безвестность, изоляцию и закрытость объекта, надёжность коммуникаций в рамках подстанции, использование внутренних проприетарных протоколов. Но всё это не решает проблему кибербезопасности ЦПС, и эти системы нуждаются в построении специализированной защиты от кибератак. С введением IEC 61850 появились риски того, что существующие меры обеспечения безопасности стали неудовлетворительными.

Суть проблемы кибербезопасности цифрового объекта, построенного с использованием IEC 61850, заключается в том, что закрытость объекта не является барьером для кибератак. В настоящее время IEC 61850 лучше всего реализован через инфраструктуру Ethernet, что из-за связи с корпоративной сетью для целей управления и мониторинга лишает создаваемую или модернизируемую систему преимуществ изоляции.

Анализ существующей нормативной базы показывает, что на настоящий момент времени нет единой и полноценной нормативно-методической базы по ЦПС, удовлетворяющей всем современным требованиям кибербезопасности. В связи с этим необходимо искать «правильные» требования, которые должны стать единым руководством по ЦПС для разработчиков, проектировщиков, и эксплуатирующих организаций, которые будут:

- определять требования кибербезопасности к проектируемым и разрабатываемым цифровым объектам;
- улучшать существующие меры по кибербезопасности при применении IEC 61850;
- улучшать механизмы кибербезопасности, используемые в существующих эксплуатируемых системах с использованием IEC 61850.

Наиболее верным из всех действующих стандартов в части мер обеспечения безопасности цифровых объектов электроэнергетики для вопросов управления доступом, обеспечения целостности и конфиденциальности данных является использование серии стандартов IEC 62351 и IEC 62443.

5. Современные тенденции развития информационной безопасности в Российской Федерации

В Российской Федерации установлены направления развития информационной безопасности, грамотная реализация которых должна позволить улучшить, модернизировать систему обеспечения информационной безопасности страны. К этим направлениям можно отнести:

- обнаружение внутренних, внешних угроз, источников их появления, а также создание эффективной системы обеспечения информационной безопасности, необходимой для решения конкретных практических задач;
- выполнение сертификационной работы традиционных и специальных программных средств, решений, комплектов прикладных приложений, средств защиты информационных данных в имеющихся и разрабатываемых автоматизированных системах управления, связи, структура которых содержит компоненты вычислительного оборудования;
- систематическая модернизация средств защиты информационных данных, улучшение уровня защищённости систем управления и связи, увеличение уровня надёжности специальных программных решений, прикладных приложений, используемого ПО;
- улучшение, модернизация структурных элементов функциональных органов систем информационной безопасности конкретных объектов, координирование их взаимодействия между собой.

Важным аспектом обеспечения кибербезопасности страны является обеспечение независимости — создание чётко выстроенной системы межведомственного взаимодействия и самостоятельной структуры для управления рисками с опорой на нормативно-правовую базу, что обеспечит полномочия и возможности для работы. Существенной проблемой становится и слабое развитие собственной аппаратной части, что ставит систему ИБ Российской Федерации в положение зависимости от иностранных поставщиков.

Независимость или степень локализации систем, жизненно важных для функционирования государства, обеспечивается за счёт:

- собственного программного обеспечения — операционных систем, систем защиты информации, SIEM-систем и других ИБ-продуктов российских разработчиков;
- собственного аппаратного комплекса — микропроцессорного оборудования, радиоэлектроники, аппаратного обеспечения;
- собственных каналов связи, чтобы поддержать «автономию» от мировой сети Интернет наиболее важных ресурсов;
- развитие квалифицированных кадров за счёт создания современного образовательного и профессионального процесса повышения качества знаний или переподготовки кадров.

Данные направления формируют облик развития информационных технологий и информационной (кибер) безопасности на ближайшие годы.

6. Законодательные инициативы в РФ

В соответствии с Энергетической стратегией Российской Федерации на период до 2035 года, принятой распоряжением Правительства Российской Федерации от 09.06.2020 № 1523-р к энергетике были отнесены следующие отрасли:

- электроэнергетика;
- нефтяная отрасль;
- газовая отрасль;
- нефтегазохимия;

- угольная отрасль.

В соответствии с пунктом № 4 «Совершенствование государственного управления и развитие международных отношений в сфере энергетики» Энергетической стратегией Российской Федерации на период до 2035 года определён комплекс ключевых мер, направленных на решение задачи обеспечения государственной, общественной и информационной безопасности в сфере энергетики, в том числе пресечение деятельности, осуществляемой специальными службами и организациями иностранных государств, террористическими и экстремистскими организациями, направленной на нанесение ущерба инфраструктуре и объектам ТЭК.

Одним из аспектов национальной безопасности по праву считается создание и развитие отечественных инфо-телекоммуникационных технологий с целью доминирования в информационном пространстве, который сегодня является приоритетным для многих стран во всем мире.

Так, в рамках объявленного руководством страны курса на импортозамещение начиная с 2014 года в рамках государственной программы «Развитие промышленности и повышение её конкурентоспособности» одной из главных задач госпрограммы заявлено снижение доли импорта продукции, в том числе используемой отечественными производителями, в нашу страну. Согласно оценкам Правительства РФ, доля импорта в промышленности в 2014 г. для станкостроения составляла 90 %, для машиностроения — 70 %, нефтегазового оборудования — 60 %, для оборудования энергетической отрасли — 50 %, сельхозмашиностроения от 50 до 90 % (в зависимости от категории продукции).

В июле 2020 г. Правительством РФ приняты законы о квотировании закупок государства (ФЗ-44) и госкомпаний (ФЗ-223) у отечественных производителей в качестве меры поддержки экономики, а в декабре утвердило перечни продукции, на которые с 2021 г. эти требования распространятся.

Помимо квотирования закупок определённой продукции государством и госкомпаниями, Правительством РФ разработаны и находятся на общественном рассмотрении требования к программному обеспечению, телекоммуникационному оборудованию и радиоэлектронной продукции, используемым на объектах критической информационной инфраструктуры, и порядка перехода на преимущественное использование российского программного обеспечения, телекоммуникационного оборудования и радиоэлектронной продукции, которые определяют следующее:

- переход на преимущественно отечественное ПО должен произойти до 1-го января 2023 г., а на отечественное железо до 1-го января 2024 г.;
- под требования попадают все объекты критической информационной инфраструктуры (КИИ) независимо от их категории значимости;
- требования касаются не только нового ПО и железа, но и уже установленного на объектах КИИ.

Курс на импортозамещение, набирающий обороты в России не уникален, а является мировым трендом. Так, например, летом 2020 г. в открытых источниках появилась новость о том, что Федеральная комиссия по регулированию энергетики США запросила у энергокомпаний информацию о наличии инфо-

телеком оборудования иностранного производства на объектах, формирующих каркас национальной энергосистемы США. Запрос ориентирован на оценку потенциальных рисков, связанных с ИБ. Президентский указ говорит о том, что выявленное используемое оборудование и программное обеспечение, произведенное за пределами США, подлежит последующему контролю, выводу из эксплуатации или замене.

- Стоит обратить внимание на то, что со стороны регуляторов, ответственных за безопасность информационных систем критически важных объектов, уделяется большое внимание и к вопросам моделирования угроз безопасности:
- в 2020 г. ФСТЭК России был опубликован проект «Методики определения угроз безопасности информации в информационных системах», описывающий порядок моделирования и определения актуальности угроз безопасности информации. Согласно новой Методике, нарушитель может обладать одним из четырех уровней потенциала (базовый, базовый повышенный, средний и высокий);
- в целях повышения эффективности и качества проведения исследований по выявлению уязвимостей ФСТЭК России разработана и утверждена 25 декабря 2020 г. новая редакция Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении, которая предназначена для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию программных, программно-технических средств технической защиты информации, средств обеспечения безопасности информационных технологий, включая защищённые средства обработки информации (далее — средства), заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств на соответствие обязательным требованиям по безопасности информации. С 1 апреля 2021 г. испытания программного обеспечения по выявлению уязвимостей и недекларированных возможностей должны проводиться в соответствии с Методикой;
- в целях оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, ФСТЭК России разработана и утверждена 05.02.2021 г. Методика оценки угроз безопасности информации, которая определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее — системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

Помимо общей специфики для объектов ТЭК существует отраслевой Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» и Федеральный закон № 116-ФЗ «О промышленной безопасности опасных производственных объектов», с которыми необходимо

согласовывать требования по информационной безопасности объектов КИИ. И, наконец, есть функциональная специфика предприятий ТЭК.

Получается, что для каждого объекта в зависимости от сектора ТЭК должна быть своя методика. Для предприятий ТЭК Минэнерго России разработало общие методические рекомендации по определению и категорированию объектов КИИ ТЭК и согласовало их с ФСТЭК России.

Минэнерго расширяет/дополняет вопросы кибербезопасности для предприятий ТЭК и помимо вышеуказанного осуществляет следующие мероприятия:

- при Минэнерго была создана межведомственная комиссия по координации обеспечения безопасности КИИ ТЭК;
- при Минэнерго в конце 2020 г. введён ведомственный центр информационной безопасности ГосСОПКА (для обмена компьютерными инцидентами с Национальным координационным центром по компьютерным инцидентам при ФСБ России);
- Минэнерго России организовывает командно-штабные тренировки и киберучения в ТЭК совместно с ФСТЭК России и ФСБ России.

Также стоит отметить, что помимо нормативных правовых актов на уровне РФ и органов исполнительной власти существуют нормативно-техническая документация, выпускаемая различными техническими комитетами, и локальные нормативные акты организаций ТЭК, регламентирующие вопросы кибербезопасности в области разработки, проектирования, создания АСДУ, АСТУ, SCADA и иных ICS систем. К таки документам относятся:

- Концепция развития релейной защиты и автоматики Электросетевого комплекса, утвержденная протоколом Правления № 356пр от 22.06.2015;
- ГОСТ Р 56939-2016. Разработка безопасного программного обеспечения. Общие требования.;
- Стандарт ПАО «ФСК ЕЭС» 2020 года. СТО 569447007-29.240.10.302-2020. Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС.

Из вышесказанного можно сделать вывод, что вопросы, связанные с обеспечением информационной и кибербезопасности являются приоритетными направлениями развития национальной безопасности для Российской Федерации.

7. Группы и профессиональные сообщества по вопросам кибербезопасности электроэнергетической отрасли в Российской Федерации

Тренд на цифровизацию электроэнергетической отрасли ставит вопрос об необходимости взаимной увязки процессов диспетчерского, технологического и автоматического управления с процессами управления кибербезопасностью. Данными вопросами в электроэнергетике занимаются такие международные и российские некоммерческие сообщества и ассоциации, как:

- CIGRE, в рамках которой существует несколько рабочих групп, занимающихся вопросами кибербезопасности устройств РЗА, в том числе и Совместная ПРГ РНК СИГРЭ B5 и D2 «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»;

- рабочая группа по вопросам безопасности объектов критической информационной инфраструктуры, созданная при Минэнерго России, в рамках которой решаются многое вопросы обеспечения информационной безопасности, в том числе разработки дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ), учитывающие особенности их функционирования именно в области ТЭК;
- НТИ Энерджинет, Центр компетенций «Кибербезопасность», который участвует в передовых проектах НТИ Энерджинет по развитию «сквозных» технологий, участвует в исследовательской и образовательной деятельности в партнерстве с крупнейшими технологическими компаниями;
- Центр НТИ МЭИ научно-прикладных исследований в области кибербезопасности автоматизированных и автоматических систем объектов электроэнергетики (изучение угроз кибербезопасности вторичных подсистем ЦПС помимо РЗА, ИЭУ разных архитектурных принципов построения;
- Ассоциация организаций цифрового развития отрасли «Цифровая энергетика», в планы которой входит участие в создании стратегии цифровой трансформации отрасли электроэнергетики.

8. Актуальные проблемы и особенности обеспечения кибербезопасности для РЗА и энергетики в целом

Релейная защита и автоматика — основа устойчивого функционирования электроэнергетической системы. РЗА в процессе цифровой трансформации должна перейти на новую цифровую платформу. При это системы РЗА имеют высокие требования к быстродействию и надёжности. Именно недостаточный уровень надёжности существующих цифровых программно-аппаратных комплексов вызывает наибольшие опасения у экспертов в области релейной защиты и автоматики.

Можно выделить наиболее актуальные вопросы, связанные с решением проблемы надёжности и информационной безопасности в условиях цифровой трансформации электроэнергетики:

- медленное освоение отечественной электронной компонентной базы;
- отечественные производители систем автоматизации и управления технологическими процессами занимают реактивную позицию в части обеспечения своих решений встроенными средствами защиты информации;
- кадровый дефицит и отсутствие необходимого объёма экспертизы в области кибербезопасности на предприятиях;
- крайне слабое внедрение регламентов безопасного цикла разработки ПО для критически важных комплексов (ГОСТ Р 56939-2016, приказ ФСТЭК № 76, IEC 62443-4-1);
- большой объём разногласий у отраслевых специалистов в вопросе моделирования угроз безопасности. Классический подход, определяемый международными стандартами и лучшими практиками в области кибербезопасности с использованием вероятностного подхода возникновения угроз, является формальным и не подходит для решения прикладных задач обеспечения надёжности и устойчивости систем управления;

- отсутствие проработанного подхода перехода с базовых мер защиты на реализацию централизации управления кибербезопасностью и выстраивания процессов, таких как управление уязвимостями, управление активами/ассетами, обнаружение, реагирование и расследование инцидентов безопасности.

9. Практические решения в области кибербезопасности РЗА

Следует отметить следующие практические шаги, сделанные в области кибербезопасности РЗА и систем управления современных объектов электроэнергетики:

- разработана модель угроз информационной безопасности для АСУ ТП, РЗА, функциональных систем и подсистем электрических подстанций и распределительных устройств электростанций генерации, задействованных в управлении электроэнергетическим режимом Единой энергетической системы;
- Центром НТИ МЭИ предложен гибридный способ моделирования угроз кибербезопасности, учитывающий отраслевую специфику электроэнергетики (при анализе последствий влияния кибератак на системы релейной защиты и автоматики цифровых и высокоавтоматизированных подстанций рекомендовано помимо классических свойств систем РЗА — чувствительность, селективность, быстродействие, надёжность — также рассматривать свойство кибербезопасности), а также положительный эффект от использования систем, основанных на знаниях, для моделирования угроз кибербезопасности подсистемы РЗА ЦПС;
- представлены перспективы практической реализации механизмов и требований безопасности на основе микроядерных ОС (таких как KasperskyOS) в современных IED устройствах для создания киберзащищённых интеллектуальных электронных устройств комплексов РЗА;
- ПАО «ФСК ЕЭС» в 2020 г. выпущен Стандарт организации для типовых решений в области информационной безопасности, в котором заложены возможности реализации принципа контролируемой деградации системы управления. К 2021 г. есть действующие проекты, которые проектируются и готовятся к внедрению по этому стандарту.

Совместное заседание решило

1. Считать решение проблемы информационной безопасности приоритетным направлением исследований в области разработки технологий оперативно-диспетчерского и оперативно-технологического управления для обеспечения устойчивого и надежного функционирования электроэнергетики России в период её цифровой трансформации.

2. Моделирование киберугроз выполнять на основе риск-ориентированных методов, при которых определяется и практически доказывается возможность возникновения наиболее критичных технологических, операционных и производственных рисков при реализации кибератак или инцидентов кибербезопасности.

3. Результаты научных исследований в области обеспечения информационной безопасности современных цифровых систем управления

возникновения наиболее критичных технологических, операционных и производственных рисков при реализации кибератак или инцидентов кибербезопасности.

3. Результаты научных исследований в области обеспечения информационной безопасности современных цифровых систем управления выносить на публичное обсуждение специалистов отрасли в рамках деятельности НП «НТС ЕЭС».

4. Рекомендовать организациям отрасли координировать планы разработки вопросов обеспечения информационной безопасности современных цифровых систем управления сетевого комплекса, объектов электроэнергетики, системы оперативно-диспетчерского и оперативно-технологического управления в целях разработки единых технических требований информационной безопасности к информационным системам управления и их апробации.

5. Рекомендовать организациям отрасли, научно-исследовательским отраслевым институтам, проектным и инжиниринговым компаниям, разработчикам и производителям аппаратуры и ПО РЗА и АСУ ТП ЦПС внедрить регламенты безопасной разработки программного обеспечения и обеспечение требований по информационной безопасности.

7. Одобрить практику создания на базе вузов научных центров НТИ, ведущих разработку вопросов обеспечения информационной безопасности цифровых систем управления, информационных систем и технологического ПО.

8. НП «НТС ЕЭС» организовать совместное рассмотрение с профильными департаментами Минэнерго России вопросов координации программ с привлечением научных исследований организаций отрасли отраслевых НИИ, центров компетенций и внедрения полученных результатов исследований для решения проблемы информационной безопасности автоматизированных систем управления электроэнергетики в условиях цифровой трансформации отрасли.

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

В. В. Молодюк

Учёный секретарь
Научно-технической коллегии
НП «НТС ЕЭС», к.т.н.

Я. Ш. Исамухамедов

Председатель секции «Проблемы надёжности и эффективности релейной защиты и средств автоматического системного управления в ЕЭС России»
НП «НТС ЕЭС», к.т.н.

А. В. Жуков

Учёный секретарь секции «Проблемы надёжности и эффективности релейной защиты и средств автоматического системного управления в ЕЭС России»
НП «НТС ЕЭС»

А. И. Расщепляев