ЭЛЕКТРОЭНЕРГЕТИКА

УДК 621.311 *DOI 10.46960/2658-6754_2022_3_49*

ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ И ИХ РЕАЛИЗАЦИЯ В ИНТЕЛЛЕКТУАЛЬНЫХ УСТРОЙСТВАХ ЦИФРОВЫХ ПОДСТАНЦИЙ

А.Л. Куликов
Нижегородский государственный технический университет им. Р.Е. Алексеева
Нижний Новгород, Россия
ORCID: 0000-0003-1092-7136 e-mail: inventor61@mail.ru

В.М. Зинин
ООО НПП «АЛИМП»
Нижний Новгород, Россия
ORCID: 0000-0001-7934-7434 e-mail: c.nemo@yandex.ru

В статье представлен обзор национального законодательства по безопасности критической информационной инфраструктуры применительно к электроэнергетике. Проанализировано текущее состояние выполнения требований национального законодательства по безопасности объектов критической информационной инфраструктуры в отрасли. Описана технология создания кроссплатформенных интеллектуальных электронных устройств для цифровых подстанций с интегрированными функциями информационной безопасности и представлена реализация таких устройств на примере устройства релейной защиты и автоматики.

Ключевые слова: информационная безопасность, в электроэнергетике, интеллектуальное электронное устройство, информационная безопасность, критическая информационная инфраструктура, цифровая подстанция.

Для цитирования: Куликов А.Л., Зинин В.М. Требования к информационной безопасности в электроэнергетике и их реализация в интеллектуальных устройствах цифровых подстанций // Интеллектуальная Электротехника. 2022. № 3. С. 49-78. DOI: 10.46960/2658-6754_2022_3_49

CYBERSECURITY REQUIREMENTS IN POWER INDUSTRY AND THEIR IMPLEMENTATION IN INTELLIGENT ELECTRONIC DEVICES OF DIGITAL SUBSTATIONS

A.L. Kulikov
Nizhny Novgorod State Technical University n.a. R.E. Alekseev
Nizhny Novgorod, Russia
ORCID: 0000-0003-1092-7136 e-mail: inventor61@mail.ru

V.M. Zinin
LLC NPP «ALIMP»
Nizhny Novgorod, Russia
ORCID: 0000-0001-7934-7434 e-mail: c.nemo@yandex.ru

An overview of the national legislation on the security of critical information infrastructure in relation to the electric power industry is given. The current state of compliance with the requirements of national legislation on the security of critical information infrastructure facilities in the industry is analyzed. The technology of creating cross-platform intelligent electronic devices for digital substations with integrated information security functions is described and an example of the implementation of such devices is given on the example of a relay protection and automation device.

Keywords: information security in the power industry, intelligent electronic device, information security, critical information infrastructure, digital substation.

For citation: A.L. Kulikov and V.M. Zinin, “Cybersecurity requirements in power industry and their implementation in intelligent electronic devices of digital substations”, *Smart Electrical Engineering*, no. 3, pp. 49-78, 2022.
DOI: 10.46960/2658-6754_2022_3_49

I. Введение

Электроэнергетическая система (ЭЭС) – одна из важнейших подсистем жизнеобеспечения. От ее надежной и безопасной работы зависит эффективное функционирование экономики всей страны. Развитие энергетики в России в последние годы вышло на качественно новый уровень благодаря внедрению современных технологий и инвестиционных программ по перевооружению всего энергетического комплекса. Большое внимание уделяется и таким проблемам, как надежность, безопасность, живучесть, энергетическая, экономическая и экологическая эффективность. Системообразующая отрасль экономики и жизнеобеспечивающая роль электроэнергетики, развитие цифровых технологий, интеллектуальных сетей и устройств делают энергетику привлекательной мишенью для атак со сто-

роны террористов, хакеров и других злоумышленников. На настоящем этапе развития электроэнергетической отрасли новые компьютерные технологии контроля, управления, измерений и передачи данных, которые используются для мониторинга режимов и управления ими, имеют целый ряд преимуществ перед традиционными технологиями. В то же время они увеличивают уязвимость при кибератаках извне, причем как на отдельные элементы ЭЭС, так и на единую национальную электрическую сеть (ЕНЭС) и единую энергосистему (ЕЭС) в целом. Поэтому внедрение новых технологий должно производиться с учетом требований защиты информации и самой информационной системы от неблагоприятных внешних воздействий. Решение проблем, связанных информационной безопасностью (ИБ) в электроэнергетике, важно не только для обеспечения энергетической безопасности, но и для стабильного состояния экономики страны, так как количество успешных кибератак злоумышленников год от года возрастает [1].

Агрессивные кибератаки направлены, в основном, на срыв технологических операций в ЭЭС. Они могут привести к разрушению системной инфраструктуры, травмам и гибели людей, нанести ущерб производствам промышленной и сельскохозяйственной продукции, транспорта, ЖКХ, а также окружающей среде и вызвать экономические и финансовые сбои и др. В «Доктрине энергетической безопасности Российской Федерации» [2], утвержденной в мае 2019 г., сформулированы основные угрозы и риски. Одной из основных трансграничных угроз обозначено «противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топливно-энергетического комплекса». Одним из основных рисков названо «несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков».

В 2022 г., согласно статистике Национального координационного центра по компьютерным инцидентам (НКЦКИ) ФСБ России [3], количество кибератак на критическую информационную инфраструктуру (КИИ) РФ существенно возросло, причем эти кибератаки носят системный, спланированный характер, что позволяет утверждать об организации и осуществлении этой противоправной деятельности специализированными структурами, управляемыми правительствами других государств.

20 мая 2022 г. состоялось заседание Совета Безопасности России, на котором были рассмотрены дополнительные меры по предотвращению последствий новых внешних угроз в сфере использования информационно-коммуникационных технологий. В ходе заседания было отмечено, что:

1) современные угрозы информационной безопасности направлены на подрыв обороноспособности страны и обеспечения правопорядка, а также ухудшение социально-экономического положения и общественно-политической ситуации в России;
2) к проведению компьютерных атак для нанесения экономического и политического ущерба нашей стране все чаще привлекаются финансово мотивированные странами Запада хакеры; для получения данных о применяемых способах и методах защиты объектов российской КИИ активно используются средства радиоэлектронной и компьютерной разведок стран НАТО;
3) в условиях экономического давления на Российскую Федерацию существенно снижается уровень доверия к программным средствам и оборудованию зарубежных производителей.

С учетом сложившейся ситуации Совет Безопасности рассмотрел и одобрил проект основ государственной политики в области обеспечения безопасности КИИ Российской Федерации, который представлен Президенту РФ для утверждения. Отметим его ключевые моменты:

- для нейтрализации упомянутых угроз документом определены цели, задачи и механизмы реализации государственной политики в ИТ-сфере;
- повышение уровня защищенности КИИ предполагается путем применения отечественных информационных технологий;
- усилия государства будут направлены на организацию НИОКР, в том числе, в области технологий искусственного интеллекта и квантовых вычислений;
- предусматривается создание конкурентоспособной электронной компонентной базы и высокотехнологичного производства, развитие государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Рассматривая отраслевой аспект ИБ применительно к единой энергосистеме Российской Федерации, важно отметить, что единичным объектом технологического управления [4, 5] является центр питания – цифровая подстанция (ЦПС) напряжением 6 кВ и выше с использованием МЭК 61850. Компоненты подсистемы ИБ таких технологических объектов должны быть интегрированы во все вторичное оборудование и АСТУ.

II. Развитие федерального законодательства для совершенствования информационной безопасности критической информационной инфраструктуры

В 2016 г. Указом Президента РФ утверждена обновленная «Доктрина информационной безопасности Российской Федерации» [6] – документ, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Под информационной сферой в Доктрине понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. «Доктрина информационной безопасности Российской Федерации» определяет национальные интересы России в информационной сфере, включающие:

- обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной жизни, а также сохранение духовно-нравственных ценностей;
- бесперебойное функционирование критической информационной инфраструктуры;
- развитие в России отрасли ИТ и электронной промышленности;
- доведение до российской и международной общественности достоверной информации о государственной политике РФ;
- содействие международной информационной безопасности.

С 01.01.2018 начал действовать принятый 26.07.2017 Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [7]. Этим законом определяются основы и принципы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации, устанавливаются права и обязанности субъектов КИИ, а также вводится институт категорирования объектов КИИ. Согласно 187-ФЗ (ст. 2, п. 8) к субъектам 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, 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, гор-

нодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей».

Вслед за принятием 187-ФЗ вышло Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [8], в котором:

- установлены порядок и сроки категорирования объектов КИИ РФ;
- установлено осуществление категорирования субъектами КИИ в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов КИИ;
- установлено, что категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ в областях (сферах), установленных п. 8 ст. 2 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

30.03.2022 Президентом РФ был подписан и вступил в силу Указ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [9], в котором предписывается в шестимесячный срок реализовать комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами КИИ отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им значимых объектах КИИ (ЗОКИИ), определить сроки и порядок перехода на преимущественное применение доверенных программно-аппаратных комплексов на ЗОКИИ, а с 01.01.2025 вводится прямой запрет на использование иностранного программного обеспечения на ЗОКИИ.

14.04.2022 Президентом РФ был подписан и вступил в силу Указ № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» [10]. Созданная Указом комиссия образована в целях выполнения возложенных на Совет Безопасности РФ задач по выработке мер, направленных на обеспечение безопасности КИИ РФ, а также по координации деятельности критически важных организаций РФ при реализации мероприятий по обеспечению технологической независимости объектов КИИ, их оснащению отечественной радиоэлектронной продукцией,

оборудованием, программно-аппаратными комплексами, включая программное и информационное обеспечение.

01.05.2022 Президентом РФ был подписан и вступил в силу Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [11], т.е. выполнять его требования необходимо с момента подписания. Указ нацелен на повышение уровня информационной безопасности критически важных организаций РФ, а именно:

- федеральных органов исполнительной власти (ФОИВ);
- высших исполнительных органов государственной власти субъектов РФ;
- государственных фондов;
- государственных корпораций и государственных компаний, созданных РФ на основании федерального закона («Росатом», «Газпром», «Русгидро», РЖД и другие);
- стратегических предприятий и стратегических акционерных обществ, перечень которых утвержден Указом Президента РФ № 1009 [12]; юридических лиц, являющимся субъектами КИИ, т. е. подпадающим под действие 187-ФЗ;
- системообразующих организаций российской экономики.

Крайне важно отметить, что данный Указ в явном виде обязывает возложить на заместителя руководителя органа (организации) полномочия по обеспечению ИБ органа (организации), в том числе, в части государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), а также создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению ИБ органа (организации). Кроме того, Указ возлагает на руководителей органов (организаций) персональную ответственность за обеспечение ИБ соответствующих органов (организаций). Также Указ устанавливает с 01.01.2025 органам (организациям) прямой запрет на использование средств 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, прямо или косвенно подконтрольные им либо аффилированные с ними. Таким образом, информационная безопасность критически важных организаций РФ перестает быть во многом их внутренним делом, а становится обязанностью, выполнение которой детально регулируется и контролируется государством.

III. Государственное регулирование и контроль обеспечения безопасности КИИ РФ

Организация различных аспектов безопасности КИИ в РФ относится к регулируемому государством виду деятельности. Эта деятельность осуществляется правопреемником Государственной технической комиссии при Президенте Российской Федерации − Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. В соответствии с Указом Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» [13], ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- противодействия иностранным техническим разведкам на территории Российской Федерации (далее – противодействие техническим разведкам);
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации);
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля.

В области обеспечения безопасности КИИ ФСТЭК России решает ряд задач, в том числе:

- реализации в пределах своей компетенции государственной политики в области обеспечения безопасности ЗОКИИ;
- осуществления государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

- организации деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;
- осуществления самостоятельного нормативно-правового регулирования вопросов;
- обеспечения безопасности ЗОКИИ;
- технической защиты информации.

Приказы ФСТЭК России, выпущенные в ходе осуществления нормативно-правового регулирования, в том числе, применительно к КИИ – документы прямого действия и обязательны к исполнению. Наиболее важными для исполнения субъектами КИИ электроэнергетики являются следующие приказы ФСТЭК России:

- Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [14];
- Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [15];
- Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [16];
- Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [17];
- Приказ ФСТЭК России №76 от 02 июня 2020 г. «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [18].

Следует отметить, что, помимо перечисленных выше документов, 10.02.2022 вступил в действие Приказ ФСТЭК № 26 «О внесении изменений в порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 года № 227» [19]. Он определяет правила кодирования объектов ЗОКИИ применительно к географическому местоположению в федеральных округах и отраслевой принадлежности. Этим приказом опреде-

лены следующие коды: 6 – энергетика; 7 – атомная энергия; 13 – топливно-энергетический комплекс (за исключением энергетики).

IV. Зрелость отраслевой нормативной базы по ИБ и КИИ в электроэнергетике и ее соответствие требованиям государственного регулятора

АО «СО ЕЭС», ПАО «ФСК ЕЭС», ПАО «Россети» относятся к стратегическим акционерным обществам, акции которых находятся в федеральной собственности, и участие РФ в управлении которыми обеспечивает стратегические интересы, обороноспособность и безопасность государства, защиту нравственности, здоровья, прав и законных интересов граждан Российской Федерации.

Кроме того, они относятся к субъектам КИИ и все центры питания ЕЭС РФ подлежат категорированию. Таким образом все технологические аппаратно-программные комплексы (РЗА и ПА, АСУ ТП, АИИСКУЭ и т.д.), которые функционируют (или создаются) для электроэнергетики, должны соответствовать, с точки зрения максимальных требований ИБ, как эксплуатирующиеся на объектах ЗОКИИ.

В соответствии с Постановлением Правительства № 127, подавляющее большинство подстанций единой национальной электрической сети (ЕНЭС), по нашему мнению, относятся к ЗОКИИ 1-й категории. Однако фактически, системы технологического управления многих этих объектов, прежде всего, РЗА и АСУ ТП построены с использованием технологий зарубежных компаний: *SIEMENS*, *ABB*, *SPRECON* и т.д. *SCADA*-системы этих объектов в качестве аппаратной платформы используют серверное оборудование на микропроцессорах *Intel*, а в качестве операционной системы *Microsoft Windows* различных версий. Автоматизированные рабочие места эксплуатационного, оперативного персонала и диспетчерских служб также используют компьютеры *Intel-Windows*.

Специализированные средства и подсистемы ИБ в технологической вычислительной сети на этих объектах зачастую либо отсутствуют, либо представлены только лишь граничными устройствами защиты периметра (*firewall*) на каналах передачи данных с центрами управления сетями (ЦУС), региональными диспетчерскими управлениями (РДУ). Также требует пристального внимания вопрос сертификации элементов АСТУ объектов ЕНЭС в системе ФСТЭК России. В соответствии с Приказом ФСТЭК России № 76 от 02.06.2020 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», элементы АСТУ объектов ЕНЭС должны быть сертифицированы по 4-му уровню доверия. Кроме того, вторичное технологическое оборудование, находящееся в эксплуатации на объектах ЕНЭС, зачастую

не в полной мере соответствует «Требованиям к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети» (утверждены Распоряжением ПАО «Россети» № 282р от 30.05.2017) [20].

В разделе 3.6. «Информационная безопасность» действующей редакции «Положения ПАО «Россети» о единой технической политике в электросетевом комплексе (решение Совета директоров ПАО «Россети», протокол заседания от 02.04.2021 № 450)» [21] определено направление развития ИБ с учетом специфики отрасли, соответствия законам РФ и требованиям государственных регуляторов. Одной из поставленных задач в данном контексте является «разработка отраслевых стандартов информационной безопасности».

Отметим, что, несмотря на значимость и перспективность разработки, базовый отраслевой СТО по ИБ в ПАО «Россети» пока не принят. При его разработке и выборе средств защиты для элементов, объектов и подсистем электроэнергетики следует учитывать, что основным активом и защищаемым объектом является, как правило, не только информация, а в первую очередь технологический процесс. И речь при этом идет о защите не от утечек информации, а от нарушений технологического процесса при возможной реализации угроз ИБ. Также в ходе разработки СТО должна быть учтена такая специфика ЕЭС России, как работа в непрерывном активном режиме, приоритет задачи сохранения функциональности АСТУ над задачей сохранения ее информационной безопасности.

В СТО должны быть определены типовые модели ИБ центров питания разных технологических поколений, разных уровней напряжения и категорий КИИ, на их основе сформулированы требования к наложенным средствам ИБ технологических объектов ЕЭС России и встроенным функциям ИБ во вторичное оборудование различного функционального предназначения, взаимодействие с ГосСОПКА и т.д. Эти категории обязательно должны сочетаться с *CIM*-моделью электроэнергетики.

Базовый отраслевой СТО по ИБ будет важным руководящим документом как для производителей различного интеллектуального оборудования и АСТУ, так и для организаций, занимающихся проектированием, реконструкцией и строительством объектов электрических сетей. Это упорядочит процессы отраслевой аттестации и выполнение обязательных требований государственных регуляторов (ФСТЭК и ФСБ), а его последующее применение повысит информационную безопасность технологических объектов электрических сетей и, как следствие, надежность электроснабжения. Система обеспечения ИБ технологических объектов ЕЭС России должна реализовываться в виде согласованных сквозных организационно-технических мероприятий и интегрированной информационной техноло-

гии, объединяющей оптимальным образом аппаратные, программные средства и организационные методы, не противоречащие требованиям государственных регуляторов. Такой системы в электроэнергетике на сегодня пока не создано, а СТО, связанные с цифровой трансформацией, к сожалению, не решают поставленной в «Технической политике…» задачи.

Указы Президента № 166 и № 250 конкретизировали сроки, в которые на объектах КИИ в электроэнергетике должны будут отказаться от иностранного ПО и оборудования.

V. Технология создания кроссплатформенных ИЭУ для ЦПС с интегрированными функциями ИБ

С учетом тенденций внедрения цифровых технологий в электроэнергетику, при участии авторов была разработана технология создания кроссплатформенных интеллектуальных электронных устройств (ИЭУ) для ЦПС с интегрированными функциями ИБ. Результатом разработки этой технологии стали аттестованные в ПАО «Россети» кроссплатформенные ИЭУ релейной защиты и автоматики для объектов электрических сетей напряжением 6-35 кВ и 110-220 кВ.

С основными функциональными возможностями и особенностями предлагаемых ИЭУ РЗА можно ознакомиться в публикациях [22-25] отраслевых журналов («Релейщик», «РУМ»). Ниже будут рассмотрены варианты реализации функций ИБ в кроссплатформенных ИЭУ, создаваемых по предложенной технологии.

Обратим внимание на развитие стандарта МЭК 61850 в направлении ИБ. На рис. 1 показаны изменения, которые инициированы международной группой разработки I*EC* 61850-8-1/*AMD*1 *ED*2 для внесения в последующую редакцию стандарта. Как можно увидеть (см. выделение пунктиром), в профиле *IEC* 61850 появился *IEC* 62351-6 «Управление энергетическими системами и связанным с этим обменом информацией. Безопасность данных и коммуникаций. Часть 6. Безопасность для *IEC* 61850». Для потоков данных, выходящих за пределы ЦПС, применение *IEC* 62351-6 будет обязательным, внутри технологической вычислительной сети ЦПС − рекомендуемым.

Дальнейшее развитие МЭК 61850 подразумевает встраивание функций ИБ в ИЭУ. Большинство выпускаемых сегодня интеллектуальных электронных устройств для ЦПС, поддерживающих МЭК 61850, не удовлетворяют в полном объеме *IEC* 62351-6. Исторически при формировании технических требований к разработке ИЭУ наличие функций ИБ не учитывалось зачастую по причине снижения быстродействия ИЭУ, что недопустимо, в частности, для ИЭУ РЗА.

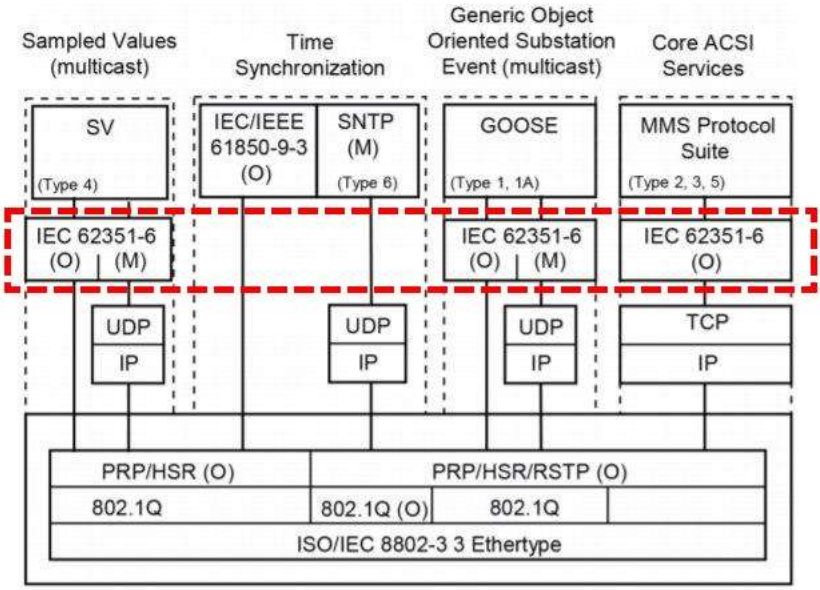

Рис. 1. Развитие стандарта МЭК 61850 в направлении ИБ

Fig. 1. Development of the IEC 61850 in the direction of cybersecurity

Современное развитие вычислительной техники характеризуется тенденцией удешевления компонентной базы (микропроцессоров, оперативной памяти, систем хранения, интерфейсных микросхем и т.д.) при росте ее надежности и производительности. В результате этого получили широкое распространение вычислительные средства промышленной автоматизации, выпускаемые серийно и имеющие высокую степень стандартизации. Также сегодня имеется возможность выбора серийно выпускаемых операционных систем для промышленных (космических, военных) условий применения, имеющих развитую систему ИБ, в том числе и сертифицированных ФСТЭК.

В технологии создания кроссплатформенных ИЭУ для ЦПС с интегрированными функциями ИБ выделяется несколько уровней абстракции (рис. 2), часть из которых представляет собой доверенную аппаратно-программную платформу, не зависящую от конкретного производителя. Использование доверенной аппаратно-программной платформы обеспечивает функции ИБ, разрабатываемого ИЭУ в соответствии с требованиями регулятора и одновременно освобождает производителя ИЭУ от трудоем-

ких процессов технического сопровождения (аттестации) аппаратного исполнения. Он может выбирать ее компоненты из государственных реестров Российского ПО и оборудования. Основные усилия производителя ИЭУ направлены на разработку, совершенствование алгоритмической базы и поддержание прикладного функционального программного обеспечения устройств, устойчивого к угрозам ИБ.

Рис. 2. Пять уровней абстракции при создании кроссплатформенного ИЭУ

Fig. 2. 5 levels of abstraction when creating a cross-platform IED

Такой подход позволяет в качестве аппаратной составляющей применять серийно выпускаемые промышленные вычислители, в основе которых лежат распространенные микропроцессоры как импортного (*Intel*, *AMD*, *ARM*, *Zhaoxin*), так и отечественного (Эльбрус, Байкал) производства, что формирует 1-й уровень абстракции. На 2-м и 3-м уровне используются серийные операционные системы, имеющие соответствующую сертификацию ФСТЭК (например, *Astra Linux*, *Alt Linux*, «Нейтрино»). Первые три уровня не зависят от конкретного производителя ИЭУ. 4-й и 5-й уровни абстракции модели ИЭУ представляют собой кроссплатформенное функциональное программное обеспечение ИЭУ и коммуникационные интерфейсы МЭК 61850.

Требования по ИБ изначально закладываются в информационную модель МЭК 61850 ИЭУ при его создании. Из представленной 5-уровневой абстракции видно, что функции ИБ распределены между 3-м и 5-м уровнями. Схематично процесс создания кроссплатформенных ИЭУ для ЦПС с интегрированными функциями ИБ показан на рис. 3.

Рис. 3. Процесс создания кроссплатформенных ИЭУ для ЦПС с интегрированными функциями ИБ

Fig. 3. Process of creating cross-platform IEDs for digital substations with integrated cybersecurity functions

ИЭУ, созданные с использованием представленной технологии, поддерживают следующие функции ИБ:

- *SSL/TLS*-шифрование для МЭК 61850-8-1 (*MMS*) между ИЭУ и другими технологическими подсистемами ЦПС, а также между ЦПС и ЦУС;
- двухфакторную аутентификацию на ИЭУ РЗА и АРМ эксплуатационного и оперативного персонала технологической вычислительной сети ЦПС при удаленном доступе к ИЭУ;

- ролевой доступ к элементам интерфейса ИЭУ в зависимости от функциональных обязанностей персонала;
- протоколирование событий безопасности на уровне отдельного ИЭУ, ЦПС и ЦУС.

Рассмотрим далее обозначенные функции ИБ подробно и проиллюстрируем примерами экранных форм ИЭУ РЗА и специализированного ПО для анализа трафика вычислительной сети. На рис. 4 и 5 представлена реализация *SSL/TLS*-шифрования для МЭК 61850-8-1 (*MMS*) между ИЭУ и другими технологическими подсистемами ЦПС. Рис. 4 демонстрирует результат захвата трафика *MMS*-пакетов ИЭУ РЗА P0101 (см. выделение рамкой) популярной программой *Wireshark* без применения *TLS*-шифрования.

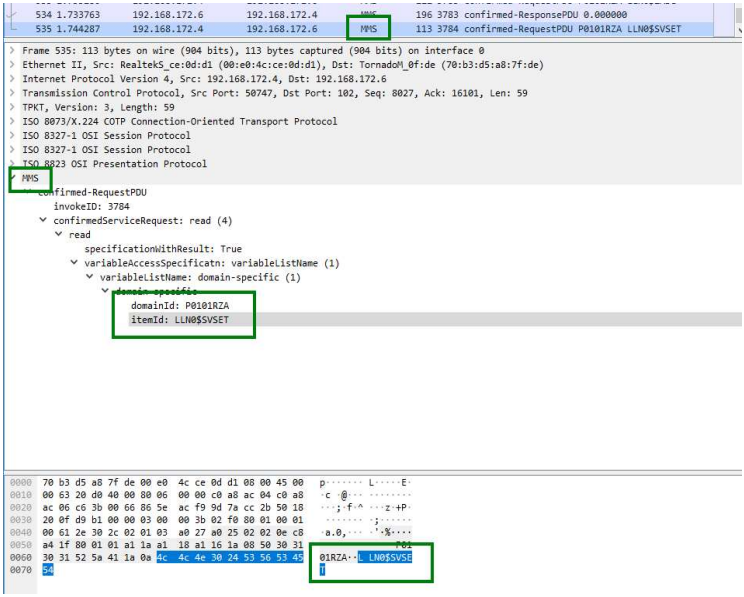

Рис. 4. Работа ИЭУ без *TLS*-шифрования MMS-пакетов

Fig. 4. IED operation without TLS encryption of MMS packets

На рис. 5 показан результат захвата *MMS*-трафика ИЭУ РЗА P0101 (см. выделение рамкой) программой *Wireshark* с включенным *TLS*-шифрованием. В отличие от рис. 4, данные *MMS* передаются в зашифрованном виде, который обеспечивает *Transport Layer Security*, и не могут быть прочитаны.

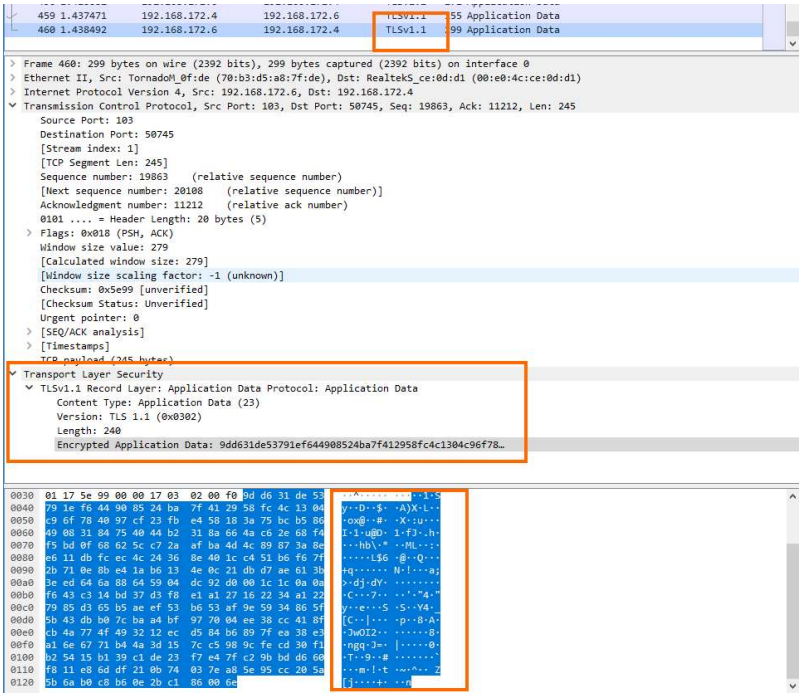

Рис. 5. Работа ИЭУ с *TLS*-шифрованием MMS-пакетов

Fig. 5. IED operation with *TLS* encryption of MMS packets

Рис. 6. Двухфакторная аутентификация с использованием *USB*-идентификатора

Fig. 6. Two-factor authentication using a USB token

Следующий пример (рис. 6) схематично демонстрирует процесс двухфакторной аутентификации на ИЭУ РЗА. Для того, чтобы зарегистрироваться на консоли ИЭУ РЗА с целью совершения каких-либо действий, сотруднику необходимо использовать индивидуальный *USB*-идентификатор, который он должен вставить в *USB*-порт на фронтальной панели ИЭУ и затем ввести свой пароль. Успешная авторизация на устройстве возможна, если сотрудник включен в список пользователей на ИЭУ с определенными правами. Иначе локальная система безопасности ИЭУ не позволит авторизоваться. При удаленном доступе к ИЭУ через вычислительную сеть ЦПС двухфакторная аутентификация осуществляется в том же порядке, только в этом случае индивидуальный *USB*-идентификатор должен быть вставлен в *USB*-порт компьютера (ноутбука). В представленном варианте используются сертифицированные ФСТЭК России на соответствие руководящему документу Гостехкомиссии России по защите от несанкционированного доступа (РД НДВ) по 2-му уровню контроля *USB*-идентификаторы Guardant ID.

Рассмотренные примеры относятся к 3-му уровню абстракции (уровень операционной системы) кроссплатформенных ИЭУ с интегрированными функциями ИБ (рис. 2). Далее продемонстрируем соответствующие возможности 5-го уровня абстракции (уровень функционального ПО) применительно к выполнению отраслевых требований по ИБ, соответствующих Распоряжению ПАО «Россети» № 282р (табл. 1).

Таблица 1.
Требования ИБ, реализованные в ИЭУ РЗА

Table 1.
Cybersecurity requirements implemented in the relay protection IED

№ п/п	Идентификатор	Наименование требования
1	*FAU_GEN*.1	Генерация данных аудита
2	*FAU_GEN*.2	Ассоциация идентификатора пользователя
3	*FAU_SAR*.1	Просмотр журналов аудита
4	*FAU_STG*.1	Защищенное хранение журнала аудита
5	*FAU_STG*.3	Действия в случае возможной потери данных аудита
№ п/п	**Идентификатор**	**Наименование требования**
6	*FAU_STG*.4	Предотвращение потери данных аудита
7	*FDP_ACC*.1	Ограниченное управление доступом
8	*FDP_ACF*.1	Управление доступом, основанное на атрибутах безопасности
9	*FIA_AFL*.1	Обработка отказов аутентификации
10	*FIA_ATD*.1	Определение атрибутов пользователя

Таблица 1 (окончание).
Требования ИБ, реализованные в ИЭУ РЗА

Table 1 (continued).
Cybersecurity requirements implemented in the relay protection IED

№ п/п	Идентификатор	Наименование требования
11	*FIA_UAU*.2	Аутентификация до любых действий пользователя
12	*FIA_UAU*.7	Аутентификация с защищенной обратной связью
13	*FIA_UID*.2	Идентификация до любых действий пользователя
14	*FMT_MSA*.1	Управление атрибутами безопасности
15	*FMT_MSA*.3	Инициализация статических атрибутов
16	*FMT_MTD*.1	Управление данными ФБО
17	*FMT_SMF*.1	Спецификация функций управления
18	*FMT_SMR*.1	Роли безопасности
19	*FTA_SSL*.1	Блокирование сеанса, инициированное функциями безопасности

Подробно остановимся на демонстрации реализации наиболее наглядных требований по ИБ (на примере ИЭУ РЗА): *FMT_SMR*.1 (Роли безопасности) и *FAU_SAR*.1 (Просмотр журналов аудита). Обратимся к табл. 2, которая была разработана, исходя из разграничения функциональных обязанностей персонала, имеющего отношение к работе с технологическим оборудованием ЦПС.

Таблица 2.
Роли безопасности в ИЭУ РЗА

Table 2.
Security roles in the relay protection IED

Название группы	Функциональные обязанности, роли	Права доступа к элементам интерфейса и функциям ИЭУ
Администратор(ы)	Представители компании-производителя и/или компании, выполняющей ПНР	Полный доступ к элементам интерфейса и параметрированию
Специалист(ы) по ИБ	Специалист по ИБ	Управление пользователями

Таблица 2 (окончание).
Роли безопасности в ИЭУ РЗА

Table 2 (continued).
Security roles in the relay protection IED

Название группы	**Функциональные обязанности, роли**	**Права доступа к элементам интерфейса и функциям ИЭУ**
Эксплуатационный персонал	Специалисты, отвечающие за эксплуатацию ИЭУ (для ИЭУ РЗА – инженеры РЗА)	Параметрирование с некоторыми ограничениями (калибровка, настройка параметров ЛВС)
Оперативный персонал	Специалисты ОВБ, диспетчерский персонал ПС	Ввод/вывод функций РЗА и автоматики, чтение осциллограмм, журнала событий
Читатель	Руководящий персонал ПС	Чтение осциллограмм, журнала событий
Специалист(ы) по АСУ ТП	Инженер по связи, инженер по ИТ	Настройка параметров ЛВС

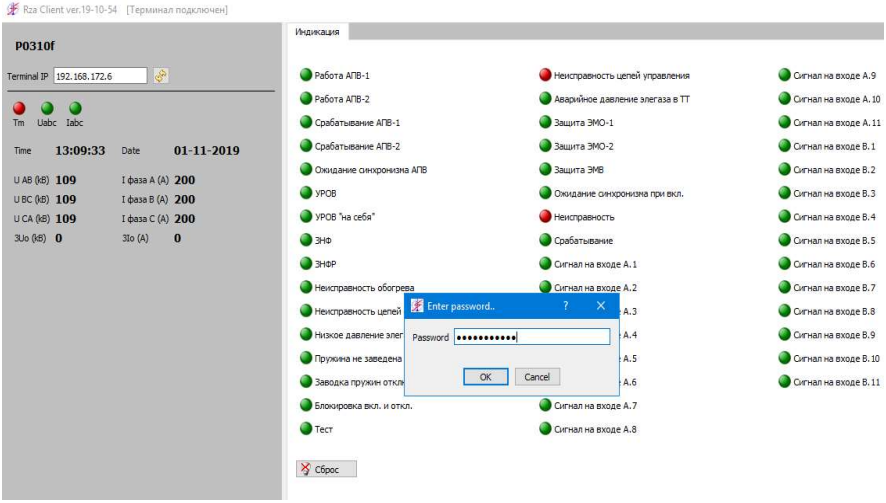

Рис. 7. Окно авторизации пользователя

Fig. 7. User Authorization Window

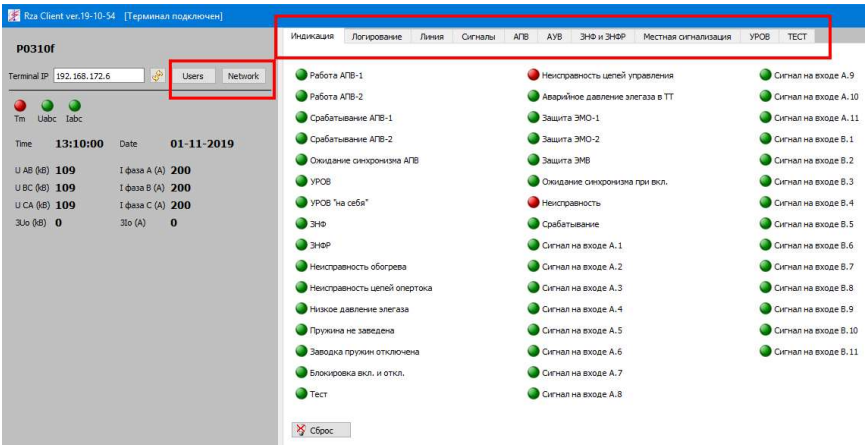

Рис. 8. Авторизовался Администратор

Fig. 8. The Administrator has logged in

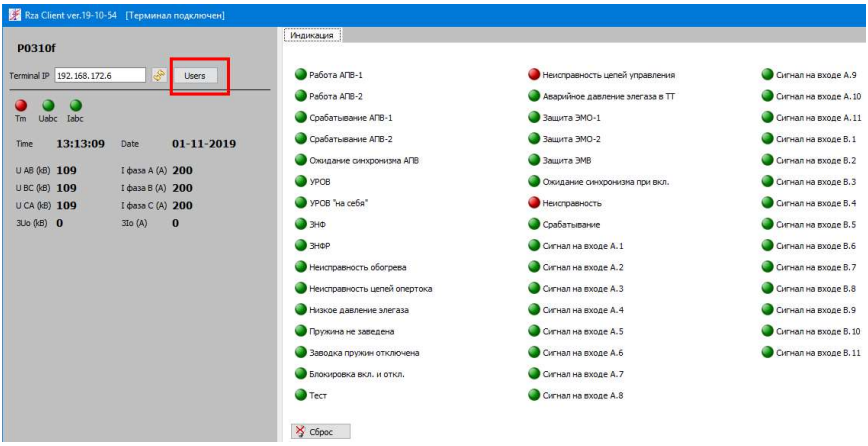

Рис. 9. Авторизовался специалист по ИБ

Fig. 9. An information security specialist has logged in

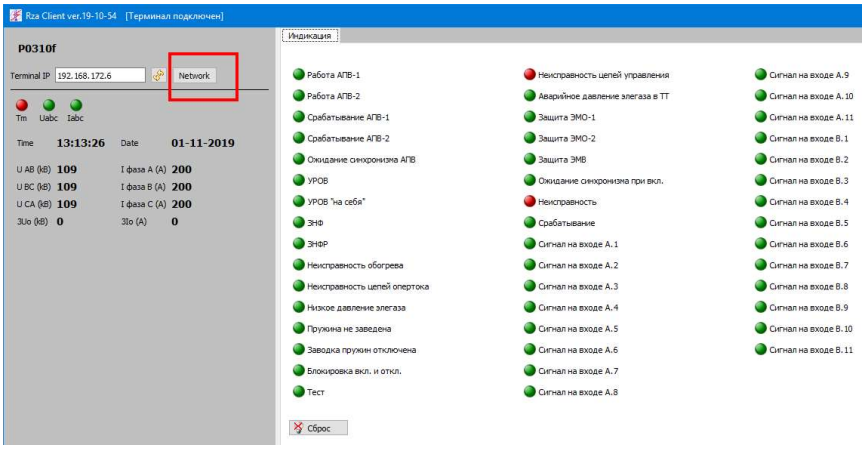

Рис. 10. Авторизовался специалист по АСУ ТП

Fig. 10. An automated control system specialist has logged in

Сценарий работы с ИЭУ начинается с авторизации пользователя (рис. 7), который включен в одну из групп (табл. 2). После обработки системой успешного запроса на вход, пользователю предоставляется интерфейс (рис. 8-10), настроенный в соответствии с его функциональными обязанностями. На рис. 8 авторизовался «Администратор», которому доступны любые действия в системе (выделение рамкой). Рис. 9 демонстрирует интерфейс пользователя «Специалист по ИБ», которому доступна на ИЭУ только возможность управления пользователями через кнопку «*Users*» (см. выделение рамкой). На этапе создания ИЭУ можно предусмотреть ограничения для «Специалиста по ИБ» на управление группой пользователей «Администраторы».

Следующий экран (рис. 10) показывает интерфейс пользователя «Специалист по АСУ ТП», функциональные обязанности которого ограничиваются настройкой параметров подключения ИЭУ к технологической вычислительной сети ЦПС («шине процесса» и «шине станции»). Доступность кнопки «*Network*» (см. выделение рамкой) дает возможность доступа к параметрированию сети, подпискам и публикациям МЭК 61850, в т.ч. для интеграции со *SCADA*-системой. На рис. 11 показан запрет на редактирование параметров ИЭУ для авторизовавшегося пользователя с правами из группы «Читатель». Элементы интерфейса (см. выделение рамкой) заретушированы серым цветом без возможности выбрать параметры или ввести их вручную и сохранить.

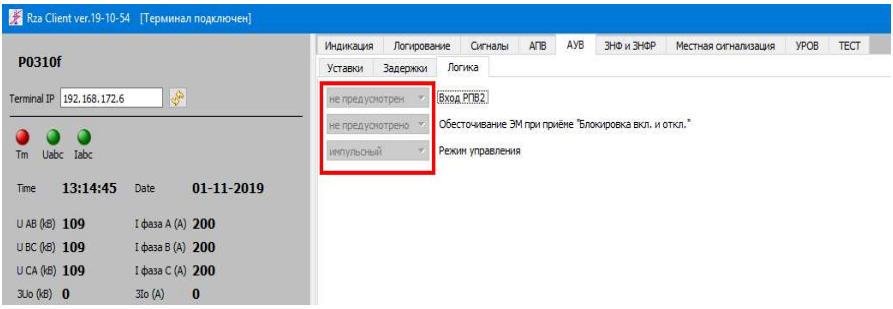

Рис. 11. Запрет на редактирование параметров ИЭУ для пользователя «Читатель»

Fig. 11. Prohibition on editing the parameters of the IED for the «Reader» role

Все действия, которые совершает пользователь при работе с ИЭУ, в том числе, события авторизации протоколируются в журнале событий ИЭУ (рис. 12).

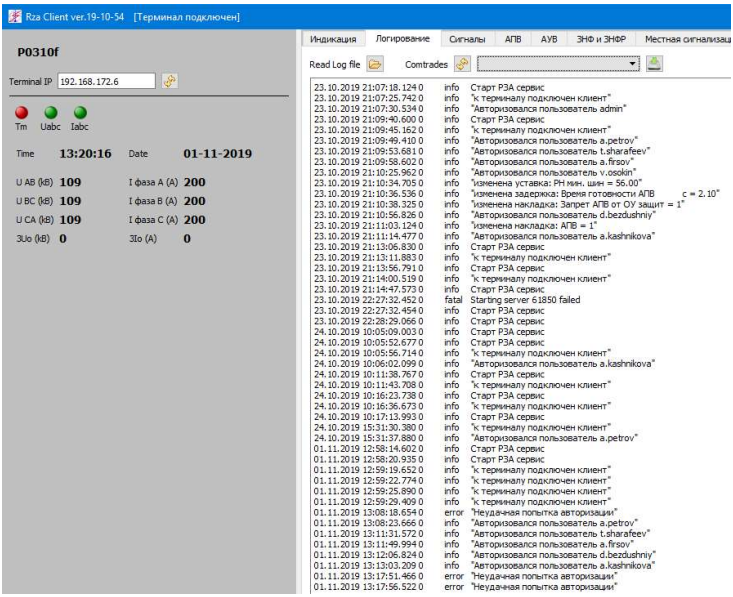

Рис. 12. Журнал событий ИЭУ (с событиями аудита)

Fig.12. IED event log (with audit events)

В статье частично показана реализация действующих отраслевых требований по ИБ в кроссплатформенных ИЭУ. В технологии создания кроссплатформенных ИЭУ большинство отраслевых требований по ИБ было предусмотрено до выхода соответствующих локальных нормативных актов [26], что подтверждает правильность реализованных технических решений.

В настоящее время кроссплатформенные ИЭУ РЗА проходят обязательную для эксплуатации на ЗОКИИ сертификацию ФСТЭК по 4 УД. В ходе прохождения сертификации аккредитованных ФСТЭК специалистами испытательных лабораторий отмечается, что разработанные в ПАО «Россети» локальные нормативные акты не в полном объеме охватывают требования государственного регулятора, которые необходимо учитывать при создании и эксплуатации объектов КИИ. Они не могут применяться в качестве основных документов при подтверждении соответствия программного и аппаратного обеспечения АСТУ (и ИЭУ РЗА в частности), в том числе их функционально-технических параметров (характеристик), требованиям по безопасности информации. Обязательная сертификация ФСТЭК не может быть подменена процедурой отраслевой аттестации ПАО «Россети».

VI. Заключение

1. Использование доверенной аппаратно-программной платформы, базирующейся на отечественных микропроцессорах и сертифицированных ФСТЭК операционных системах для создания кроссплатформенных ИЭУ различного функционального назначения АСТУ ЦПС, является перспективным вариантом снижения технологической зависимости электроэнергетической отрасли РФ и минимизации угроз и рисков, изложенных в обновленной «Доктрине энергетической безопасности Российской Федерации».

2. Импортозамещение должно проходить, в том числе, через реализацию программы НИОКР, отработку типовых технических решений и нормативных документов (СТО) по их завершении. Определяющим критерием должна быть не стоимость, а технологическая нейтральность и минимизация зависимости от импортных составляющих, т.к. для компаний, одним из учредителей, которых выступает государство, это является решением важнейшей стратегической государственной задачи.

3. Указы Президента № 166 от 30.03.2022 и № 250 от 01.05.2022 конкретизировали сроки, в которые на объектах КИИ в электроэнергетике должны отказаться от иностранного ПО и оборудования. Основное федеральное законодательство сформировано и обязывает компании с государственным участием системно проводить такую работу. Информационная безопасность критически важных организаций РФ перестает быть их внут-

ренним делом, а становится обязанностью, выполнение которой регулируется и контролируется государством.

4. С учетом кардинального изменения внешнеполитической ситуации в 2022 г. и изменения законодательства РФ единая техническая политика в электросетевом комплексе, как основополагающий документ, должна быть пересмотрена в части усиления задачи импортозамещения, а ее отдельные разделы, такие как «Информационная безопасность» уточнены, прежде всего, с учетом категорирования центров питания как объектов КИИ.

5. Необходимо активизировать работу по разработке, обсуждению и принятию базового отраслевого СТО по информационной безопасности.

Поступила в редакцию 30.08.2022
Received 30.08.2022

Библиографический список

[1] Папков Б.В., Куликов А.Л., Осокин В.Л. Киберугрозы и кибератаки в электроэнергетике. Н. Новгород: НИУ РАНХиГС, 2017. – 78 с.
[2] Указ Президента Российской Федерации № 216 от 13.05.2019 г. «Об утверждении Доктрины энергетической безопасности Российской Федерации».
[3] Приказ Федеральной службы безопасности Российской Федерации № 366 от 24.07.2018 «О Национальном координационном центре по компьютерным инцидентам».
[4] СТО 56947007-29.240.10.248-2017. Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ (НТП ПС). Введ. 2017-08-25. М.: ПАО «ФСК ЕЭС», 2017. – 135 с.
[5] СТО 34.01-21-004-2019. Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ. Введ. 2019-03-29. М.: ПАО «Россети», 2019. – 114 с.
[6] Указ Президента Российской Федерации № 646 от 05.12.2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации».
[7] Федеральный закон № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации».
[8] Постановление Правительства РФ № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

[9] Указ Президента Российской Федерации № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
[10] Указ Президента Российской Федерации № 203 от 14.04.2022 г. «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации».
[11] Указ Президента Российской Федерации № 250 от 01.05.2022 г. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
[12] Указ Президента Российской Федерации № 1009 от 04.08.2004 г. «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ».
[13] Указ Президента Российской Федерации № 1085 от 16.08.2004 г. «Вопросы Федеральной службы по техническому и экспортному контролю».
[14] Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
[15] Приказ ФСТЭК России от 06.12.2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».
[16] Приказ ФСТЭК России № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
[17] Приказ ФСТЭК России № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
[18] Приказ ФСТЭК России №76 от 02 июня 2020 г. «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».
[19] Приказ ФСТЭК России № 26 от 10 февраля 2022 г. «О внесении изменений в порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный Приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 года № 227».
[20] Распоряжение ПАО «Россети» № 282р от 30.05.2017 г. «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети».

[21] Решение Совета директоров ПАО «Россети» (протокол заседания от 02.04.2021 № 450) «Положение ПАО «Россети» о единой технической политике в электросетевом комплексе».
[22] Куликов А.Л., Зинин В.М., Петров А.А. Обеспечение кибербезопасности в технологии «Цифровой подстанции» с учетом импортозамещения // Науч.-практ. конф. «Релейная защита и автоматика энергосистем 2017», Апрель 25-28, 2017, Санкт-Петербург, Россия.
[23] Куликов А.Л., Зинин В.М., Шарафеев Т.Р. Принципы реализации кибербезопасных решений для кроссплатформенных интеллектуальных электронных устройств (ИЭУ) в составе цифровых подстанций (ЦПС) // Электроэнергетика в национальных проектах, Рогалева Н.Д. М.: Изд-во МЭИ, 2020. – С. 167-177.
[24] Куликов А.Л., Зинин В.М., Шарафеев Т.Р. Принципы реализации кроссплатформенных цифровых подстанций // Релейщик. 2019. № 2 (34). С. 22-26.
[25] Зинин В.М. Актуальные решения НИПОМ с учетом доктрины энергетической безопасности РФ // РУМ. 2020. № 6 (596). С. 38-45.
[26] Распоряжение ПАО «Россети» № 62 от 28.02.2022 «Требования по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики».

References

[1] B.V. Papkov, AL. Kulikov and V.L. Osokin, *Kiberugrozy i kiberataki v elektroenergetike [Cyber threats and cyber-attacks in the electric power industry].* N. Novgorod: NRU RANEPA, 2017 (in Russian).
[2] Decree of the President of the Russian Federation no. 216 dated May 13, 2019 *"Ob utverzhdenii Doktriny energeticheskoj bezopasnosti Rossijskoj Federacii [On Approval of the energy security Doctrine of the Russian Federation]"* (in Russian).
[3] Order of the Federal Security Service of the Russian Federation no. 366 dated July 24, 2018 "*O Nacional'nom koordinacionnom centre po komp'yuternym incidentam» [On the National coordination center for computer incidents]"* (in Russian).
[4] *Normy tekhnologicheskogo proektirovaniya podstancij peremennogo toka s vysshim napryazheniem 35-750 kV (NTP PS) [Norms of technological design of AC substations with the highest voltage of 35-750 kV (NTP PS)],* STO 56947007-29.240.10.248-2017, August 2017 (in Russian).
[5] *Cifrovoj pitayushchij centr. Trebovaniya k tekhnologicheskomu proektirovaniyu cifrovyh podstancij napryazheniem 110-220 kV i uzlovyh cifrovyh podstancij napryazheniem 35 kV [Digital feeding center. Requirements for the technological design of digital substations with a voltage of 110-220 kV and nodal digital substations with a voltage of 35 kV]*, STO 34.01-21-004-2019, March 2019 (in Russian).
[6] Decree of the President of the Russian Federation no. 646 dated Dec. 05, 2016 *"Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii [On Approval of the information security Doctrine of the Russian Federation]"* (in Russian).
[7] Federal Law no. 187-FZ of July 26, 2017 *"O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [On the security of the critical information infrastructure of the Russian Federation]"* (in Russian).

[8] Decree of the Government of the Russian Federation no. 127 of Feb. 8, 2018 *"Ob utverzhdenii Pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij [On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values]"* (in Russian).

[9] Decree of the President of the Russian Federation no. 166 of March 30, 2022 *"O merah po obespecheniyu tekhnologicheskoj nezavisimosti i bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation]"* (in Russian).

[10] Decree of the President of the Russian Federation no. 203 of April 14, 2022 *"O Mezhvedomstvennoj komissii Soveta Bezopasnosti Rossijskoj Federacii po voprosam tekhnologicheskogo suvereniteta gosudarstva v sfere razvitiya kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [On the Interdepartmental Commission of the Security Council of the Russian Federation on the technological sovereignty of the state in the development of the critical information infrastructure of the Russian Federation]"* (in Russian).

[11] Decree of the President of the Russian Federation no. 250 dated May 1, 2022 *"O dopolnitel'nyh merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii [On additional measures to ensure the information security of the Russian Federation]"* (in Russian).

[12] Decree of the President of the Russian Federation no. 1009 dated Aug. 04, 2004 *"Ob utverzhdenii perechnya strategicheskih predpriyatij i strategicheskih akcionernyh obshchestv [On approval of the list of strategic enterprises and strategic joint-stock companies]"* (in Russian).

[13] Decree of the President of the Russian Federation no. 1085 dated Aug. 16, 2004 *«Voprosy Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu [Issues of the Federal Service for technical and export control]"* (in Russian).

[14] Order of the FSTEC of Russia no. 31 dated March 14, 2014 *"Ob utverzhdenii Trebovanij k obespecheniyu zashchity informacii v avtomatizirovannyh sistemah upravleniya proizvodstvennymi i tekhnologicheskimi processami na kriticheski vazhnyh ob"ektah, potencial'no opasnyh ob"ektah, a takzhe ob"ektah, predstavlyayushchih povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudej i dlya okruzhayushchej prirodnoj sredy [On approval of the Requirements for ensuring the protection of information in automated control systems for production and technological processes at critically important facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to life and health people and for the natural environment]"* (in Russian).

[15] Order of the FSTEC of Russia no. 227 dated Dec. 6, 2017 *"Ob utverzhdenii poryadka vedeniya reestra znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [On approval of the procedure for maintaining a register of significant objects of the critical information infrastructure of the Russian Federation]"* (in Russian).

[16] Order of the FSTEC of Russia no. 235 dated Dec. 21, 2017 *«Ob utverzhdenii trebovanij k sozdaniyu sistem bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i obespecheniyu ih funkcionirovaniya [On approval of the Requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning]"* (in Russian).

[17] Order of the FSTEC of Russia no. 239 dated Dec. 25, 2017 *"Ob utverzhdenii Trebovanij po obespecheniyu bezopasnosti znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [On approval of the Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation]"* (in Russian).

[18] Order of the FSTEC of Russia no. 76 dated June 02, 2020 *"Ob utverzhdenii Trebovanij po bezopasnosti informacii, ustanavlivayushchie urovni doveriya k sredstvam tekhnicheskoj zashchity informacii i sredstvam obespecheniya bezopasnosti informacionnyh tekhnologij [On approval of the Requirements for information security, establishing levels of trust in technical information protection tools and information technology security tools"]* (in Russian).

[19] Order of the FSTEC of Russia no. 26 dated Feb. 10, 2022 *"O vnesenii izmenenij v poryadok vedeniya reestra znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, utverzhdyonnyj Prikazom Federal'noj sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 6 dekabrya 2017 goda № 227 [On amendments to the procedure for maintaining the register of significant objects of critical information infrastructure of the Russian Federation, approved by Order of the Federal Service for Technical and Export Control dated December 6, 2017 no. 227]"* (in Russian).

[20] Order of PJSC Rosseti no. 282r dated May 30, 2017 *"Ob utverzhdenii trebovanij k vstroennym sredstvam zashchity informacii avtomatizirovannyh sistem tekhnologicheskogo upravleniya elektrosetevogo kompleksa gruppy kompanij «Rosseti» [On approval of the requirements for built-in information security tools for automated technological control systems of the electric grid complex of the "Rosseti" group of companies]"* (in Russian).

[21] Decision of the Board of Directors of PJSC Rosseti (a protocol of a meeting no. 450 dated Apr. 2, 2021) *"Polozhenie PAO «Rosseti» o edinoj tekhnicheskoj politike v elektrosetevom komplekse [Regulations of PJSC Rosseti on a unified technical policy in the electric grid complex]"* (in Russian).

[22] A.L. Kulikov, V.M. Zinin and A.A. Petrov, Obespechenie kiberbezopasnosti v tekhnologii «Cifrovoj podstancii» s uchetom importozameshcheniya [Ensuring cybersecurity in the "Digital Substation" technology, taking into account import substitution], in proc. *Nauchyu-praktyu konf. «Relejnaya zashchita i avtomatika energosistem 2017» [Nauchyu-praktyu conf. "Relay protection and automation of power systems 2017"]*, April 25-28, 2017, St. Petersburg, Russia (in Russian).

[23] A.L. Kulikov, V.M. Zinin and T.R. Sharafeev, "Principy realizacii kiberbezopasnyh reshenij dlya krossplatformennyh intellektual'nyh elektronnyh ustrojstv (IEU) v sostave cifrovyh podstancij (CPS) [Principles for the implementation of cybersecurity solutions for cross-platform intelligent electronic devices (IEDs) as part of digital substations (DPS)]", in *Elektroenergetika v nacional'nyh proektah [Power industry*

in national projects], N.D. Rogaleva, Moscow: MPEI, 2020, pp. 167-177 (in Russian).
[24] A.L. Kulikov, V.M. Zinin and T.R. Sharafeev, "Principy realizacii krossplatformennyh cifrovyh podstancij [Principles for the implementation of cross-platform digital substations]", *Relejshchik [Relay operator],* vol. 2, no. 34, pp. 22-26, 2019 (in Russian).
[25] V.M. Zinin, "Aktual'nye resheniya NIPOM s uchyotom doktriny energeticheskoj bezopasnosti RF [Actual decisions of NIPOM taking into account the doctrine of energy security of the Russian Federation]", *RUM*, vol. 6 (596), pp. 38-45, 2020 (in Russian).
[26] Order of PJSC Rosseti no. 62 dated Feb. 28, 2022 *"Trebovaniya po obespecheniyu bezopasnosti informacii mikroprocessornyh ustrojstv relejnoj zashchity i avtomatiki [Requirements for ensuring the security of information of microprocessor-based relay protection and automation devices]"* (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ
INFORMATION ABOUT THE AUTHORS

Куликов Александр Леонидович, доктор технических наук, профессор Нижегородского государственного технического университета им. Р.Е. Алексеева, г. Нижний Новгород, Российская Федерация

Alexander L. Kulikov, D. Sci. (Eng.), professor of the Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Nizhny Novgorod, Russian Federation

Зинин В.М., заместитель генерального директора по ИБ ООО НПП «АЛИМП», г. Нижний Новгород, Российская Федерация

Vladimir M. Zinin, deputy director general for information security LLC NPP «ALIMP», Nizhny Novgorod, Russian Federation