Обеспечение кибербезопасности в технологии «Цифровой подстанции» с учетом импортозамещения

А.Л. Куликов НГТУ им. Р.Е. Алексеева, В.М. Зинин ОАО «НИПОМ», А.А. Петров ОАО «НИПОМ»
Российская Федерация

Контактные лица:
ФИО: Куликов Александр Леонидович
Организация: НГТУ им. Р.Е. Алексеева
Почтовый адрес: 603950 Россия, г. Нижний Новгород, Сормовское шоссе д.12 кв.19.
e-mail: inventor61@mail.ru
тел.: +79107912656
ФИО: Зинин Владимир Михайлович
Организация: ОАО «НИПОМ»
Почтовый адрес: 606007, Россия, Нижегородская область, г. Дзержинск, ул. Зеленая, д.10
e-mail: v.zinin@nipom.ru
тел: +79621741464
ФИО: Петров Антон Александрович
Организация: ОАО «НИПОМ»
Почтовый адрес: 606007, Россия, Нижегородская область, г. Дзержинск, ул. Зеленая, д.10
e-mail: a.petrov@nipom.ru
тел: +79625182413

Ключевые слова: релейная защита, импортозамещение, кибербезопасность, надежность электроснабжения, АСУ ТП, цифровая подстанция, МЭК 61850, микропроцессор «Эльбрус»

Введение.

В 1983 году Дэвид Кан [1] сказал: «Великая держава – это страна, которая владеет ядерными технологиями, ракетными технологиями и криптографией». И сегодня по прошествии более 30 лет немногие государства обладают технологиями разработки и производства собственных микропроцессоров, криптографии и шифрования. Трансграничные ограничения запрещают передачу технологий криптографии и шифрования. Применительно к электроэнергетической отрасли, где используются элементы систем технологического управления, разработанные в разных странах, эти законодательные ограничения становятся наиболее чувствительными с ростом уровня автоматизации объектов электроэнергетики.

В открытом доступе периодически публикуются и актуализируются документы о кибератаках на критическую инфраструктуру. Например, в одном из последних отчетов компании Panda Security, так называемой «белой книге» (white book) «Критическая инфраструктура: кибератаки на основы современной экономики» собраны в хронологическом порядке (начиная с 1983 года) наиболее существенные кибератаки в мире на объекты критической инфраструктуры. Одной из последних кибератак (конец 2015 года) стало нарушение работы части энергосистемы Украины, в результате которого свыше 600 тысяч жителей остались без электричества.

Сегодня наряду с физической безопасностью защита критической инфраструктуры от кибератак становится одним из основных вопросов национальной безопасности.

Государственная политика в области кибербезопасности в электроэнергетической отрасли.

Мировые события последних 3-4 лет, связанные с ростом различных компьютерных инцидентов, заставляют пересмотреть отношение со стороны государства к кибербезопасности объектов электроэнергетики и, прежде всего, электрических подстанций магистральных сетей и межсистемных связей, т.к. с точки зрения нанесения ущерба именно они представляют наибольший интерес для злоумышленников.

В декабре 2016 года практически синхронно были опубликованы в США и Российской Федерации два официальных документа: «Объединенная стратегия США и Канады по кибербезопасности и устойчивости

электрических сетей» [2] и обновленная «Доктрина информационной безопасности Российской Федерации» [3]. Подобная работа проводится в Европейском Союзе, Китае и других странах.

В обновленной «Доктрине информационной безопасности Российской Федерации» развиты положения Стратегии национальной безопасности РФ, касающиеся:

- возрастающего противоборства в глобальном информационном пространстве;
- угроз нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры РФ;
- деятельности, связанной с использованием информационных и коммуникационных технологий в экстремистской деятельности;
- а также импортозамещения и снижения критической зависимости от зарубежных технологий и промышленной продукции.

Доктрина провозглашает ликвидацию зависимости от иностранных информационных технологий частью стратегии информационной безопасности Российской Федерации.

В целях реализации «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом России 5 декабря 2016 года, в рамках которой защита объектов критической информационной инфраструктуры (КИИ) определяется как одна из стратегических целей, в январе 2017 года Правительством РФ был внесен проект федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации», определяющий основные принципы госрегулирования в сфере защиты критической информационной инфраструктуры страны от хакерских атак. Этот законопроект был рекомендован Комитетом Государственной Думы по энергетике к принятию и принят в первом чтении 27 января 2017 года.

В пояснительной записке к законопроекту указано: «Законопроектом устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры, полномочия государственных органов РФ в области обеспечения безопасности критической информационной инфраструктуры, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами критической информационной инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов». Согласно законопроекта «к критической инфраструктуре относятся информационные системы и телекоммуникационные сети госорганов, автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.»

«Цифровые подстанции» в единой энергосистеме России.

Единицей технологического управления в ЕНЭС РФ (единая национальная электрическая сеть) является подстанция. Перечислим ее основные вторичные подсистемы:

- технологическая связь и передача данных;
- управление противоаварийной автоматикой;
- релейная защита и автоматика;
- АСУ ТП;
- учет электроэнергии и мощности (АИИСКУЭ);
- видеонаблюдение, пожарная и охранная сигнализации;
- подсистема единого времени, синхронизированная с глобальным временем.

Уровень автоматизации вторичных подсистем на подстанциях ЕНЭС различен и обычным является одновременная эксплуатация подсистем разных поколений, работающих по различным протоколам. Зачастую многие специалисты даже эти объекты называют цифровыми подстанциями. Тем не менее в принятой ПАО «ФСК ЕЭС» «Концепции интеллектуальной электроэнергетической системы России с активно-адаптивной сетью» (ИЭС ААС) [4] и в соответствии с «Положением ОАО «Россети» о Единой технической политике в электросетевом комплексе» [5] применительно к цифровым подстанциям декларируется соответствие стандарту МЭК 61850. Исходя их этого дадим определение цифровой подстанции.

Цифровая подстанция (ЦПС) – это электрическая подстанция (ПС), система технологического управления которой построена на базе стандарта МЭК 61850 с использованием в качестве первичных измерителей цифровых трансформаторов тока (ЦИТТ) и напряжения (ЦИТН), а также выносных устройств сопряжения с объектом (УСО) и интеллектуальных электронных устройств (IED). Отличительной особенностью ЦПС является локализация кабелей связи и управления в силовом оборудовании и/или в шкафах выносных УСО, ЦИТТ, ЦИТН, а для передачи информации используется сеть с коммутацией пакетов Ethernet, настроенная специальным образом (шина процесса и шина подстанции в терминологии МЭК 61850).

Таким образом, наличие вторичных подсистем, приведенных выше для обычной подстанции справедливо и для ЦПС, но принципиальным различием является использование в ЦПС протоколов стандарта МЭК 61850 (SV, GOOSE, MMS).

Аппаратно-программная платформа «Эльбрус» как основа ЦПС в киберзащищенном исполнении.

Специалистам, профессионально занимающимся вопросами информационной безопасности (кибербезопасности) понятно, что основными возможными источниками так называемых «закладок» (backdoors), позволяющих перехватить управление информационной системой являются: микросхема центрального процессора (ЦП); микросхема контроллера периферийных интерфейсов (КПИ); базовая система ввода-вывода (BIOS). Возникает резонное беспокойство, что, даже если производство импортного оборудования локализовано в РФ или производитель оборудования является отечественным, то где, как и кем изготавливаются ЦП, КПИ и программируется BIOS?

С учетом сказанного сформулируем основные требования к аппаратно-программной платформе для ЦПС в кибербезащищенном исполнении. Она должна:

• создаваться, руководствуясь национальной политикой, на российской доверенной аппаратно-программной платформе, ключевые компоненты которой (операционная система, микропроцессор, контроллер периферийных интерфейсов, базовая система ввода-вывода) разработаны в РФ, силами российских специалистов и имеют полную конструкторскую документацию;

• учитывать положения стандартов, разработанных группой IEC TC57: IEC 61850, IEC60870, IEC 62351 в части безопасности коммуникационных протоколов, а также требования стандарта INL Cyber Security Procurement Language 2008, серии стандартов ISO/IEC 27000 в части общих принципов обеспечения безопасности цифровых систем управления и ГОСТ-Р МЭК 62443-3-2013;

• использовать Российские ГОСТ-ированные алгоритмы шифрования и криптозащиты, которые встраиваются в каждое IED, УСО, MU, терминалы РЗА, АСУ ТП;

• обладать экспортным потенциалом.

С точки зрения использования криптографии и шифрования применительно к протоколам SV, GOOSE и MMS стандарта МЭК 61850 следует говорить в первую очередь об обеспечении контроля целостности Ethernet-кадров (SV, GOOSE) и TLS-шифровании (MMS), а также о ролевом доступе к элементам управления ЦПС в зависимости от функциональных обязанностей.

Особенность построения технологических систем управления в электроэнергетике заключается в том, что применение криптографии и шифрования в них не должно снижать производительность, т.к. длительность переходных (аварийных) процессов составляет десятки микросекунд. Во многих применяемых сегодня микроконтроллерах встраивание перечисленных выше элементов кибербезопасности либо не предусмотрено изначально разработчиком, либо невозможно, т.к. их встраивание не позволит обеспечить требуемое быстродействие. Для того, чтобы элементы криптографии и шифрования могли быть встроены в элементы «интеллекта» ЦПС с минимальными трудозатратами и затратами на сертификацию, «интеллект» ЦПС должен использовать не узкоспециализированные контроллеры (в подавляющем большинстве импортного производства), а универсальные микропроцессоры с операционными системами, для которых соответствующие криптографические модули уже разработаны.

С учетом импортозамещения в полной мере сформулированным требованиям отвечает российская аппаратно-программная платформа «Эльбрус» ПАО «ИНЭУМ им. И.С. Брука» и АО «МЦСТ», выпускающих средства автоматизации для оборонно-промышленного комплекса и космической отрасли [6].

Таблица 1

	«Эльбрус-4С» (1891ВМ8Я) - базовый 64-разрядный микропроцессор для серийно выпускаемого сервера, содержащего четыре процессора и два южных моста КПИ-1, а также для других схемотехнических решений. Также процессор используется и в рабочих станциях. Оборудование на базе «Эльбрус-4С» в составе ЦПС подходит для использования в качестве серверов АСУ ТП и автоматизированных рабочих мест оперативного, эксплуатационного и инженерного персонала.
	«Эльбрус-1С+» (1891ВМ11Я) — экономичный 64-разрядный микропроцессор с встроенным графическим ядром с поддержкой аппаратного ускорения 3D-графики по стандарту OpenGL 3.1. «Эльбрус-1С+» поддерживает работу с южным мостом КПИ-2 (контроллером периферийных интерфейсов 2-го поколения). Малое энергопотребление (не больше 10 Вт) позволяет применять микропроцессор в персональных компьютерах, ноутбуках, тонких клиентах, промышленной автоматике и встраиваемых системах. Применительно к ЦПС может быть использован в качестве «ядра» для IED, MU, терминалов РЗА, контроллеров присоединений.

Технические решения, выполненные на базе аппаратно-программной платформы «Эльбрус», эксплуатируются в жестких с точки зрения температуры окружающей среды, влажности, ЭМС и помех

различного характера, механических, химических воздействий, вибраций условиях и демонстрируют высокую надежность. Среди серийно выпускаемых есть модули, относящиеся к аппаратуре общего применения вида 1, работающей в режиме непрерывного длительного применения, невосстанавливаемой в процессе эксплуатации и необслуживаемой в соответствии с ГОСТ РВ 20.39.303-98. «Ядром» решений являются микропроцессоры «Эльбрус-4С» и «Эльбрус-1С+» (Таблица 1) и разработанные для них контроллеры периферийных интерфейсов (КПИ-1) первого и второго (КПИ-2) поколения соответственно.

Операционная система реального времени ОС «Эльбрус» обеспечивает многозадачный и многопользовательский режимы работы. Для неё разработаны особые механизмы управления процессами, виртуальной памятью, прерываниями, сигналами, синхронизацией, поддержка тегированных вычислений.

Вычислительные комплексы на базе «Эльбрус-4С» позволяют осуществлять межмашинные обмены данными через каналы ioLVDS. При объединении машин в кластеры через межмашинные каналы обмена ioLVDS используется драйвер виртуального Ethernet-адаптера, который поддерживает работу библиотеки MPI (Message Passing Interface – интерфейс передачи сообщений), доработанной в части осуществления удалённого прямого доступа к памяти (RDMA) через Ethernet-каналы. Данная технология позволяет строить кластеры с возможностью межмашинных обменов на скорости порядка 10 Гбит/с и минимальными задержками.

Базовые средства поддержки интерфейса пользователей в составе ОС «Эльбрус», а именно: интерфейс командной строки; архивация/сжатие файлов; ассемблеры, трансляторы, компиляторы, компоновщики (редакторы связей), сборщики, препроцессоры, отладчики, текстовые редакторы, библиотеки подпрограмм, средства управления версиями, средства документирования; планировщик заданий; поддержка графического пользовательского интерфейса Xorg, а также набор различных вспомогательных библиотек, в том числе GTK+ и Qt.

Отдельно следует отметить кибербезопасность универсальных микропроцессоров «Эльбрус». Они обеспечивают уникальные эффективные средства защищенного исполнения программ на базе аппаратных тегов и контекстной межмодульной защиты данных за счет поддержки со стороны аппаратуры, операционной системы и систем языкового программирования – компиляторов, редакторов связи, отладчиков. Таким образом технологические возможности платформы создают основу для защиты от компьютерных вирусов. В ядро ОС «Эльбрус» встроен комплекс средств защиты информации (КСЗИ) от несанкционированного доступа (НСД). Функционирование КСЗИ ОС «Эльбрус» обеспечивает требуемый уровень защиты информации от НСД при использовании в составе ЦПС. КСЗИ от НСД ОС «Эльбрус» предоставляет возможность применять средства вычислительной техники серии «Эльбрус» для построения автоматизированных систем, отвечающих требованиям 2-го класса защищённости от НСД РД Гостехкомиссии при президенте РФ и позволяющих проводить сертификацию программного обеспечения по 2-му уровню контроля недекларированных возможностей, в соответствии с РД Гостехкомиссии при Президенте РФ.

ЦПС в киберзащищенном исполнении с терминалами РЗА и SCADA-системой на аппаратно-программной платформе «Эльбрус» была впервые представлена на выставке «Электрические сети России – 2016» [7].

Выводы.

1. Для проектирования ЦПС с учетом требований импортозамещения и кибербезопасности целесообразно и обосновано применение аппаратно-программной платформы «Эльбрус».
2. Технологическая зрелость аппаратно-программной платформы «Эльбрус» для использования в ЦПС подтверждается решениями, представленными на выставке «Электрические сети России- 2016», например, компанией ОАО «НИПОМ».

Литература.

1. Kahn, D., Kahn on Codes, Macmillan Publishing Co., New York, NY, 1983
2. JOINT UNITED STATES-CANADA ELECTRIC GRID SECURITY AND RESILIENCE STRATEGY (https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
3. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646 http://kremlin.ru/acts/news/53418).
4. «Концепция интеллектуальной электроэнергетической системы России с активно-адаптивной сетью» под ред. Фортова В.Е, Мастерова А.А., ОАО «ФСК ЕЭС», Москва 2012 г.
5. «Положение ОАО «Россети» о Единой технической политике в электросетевом комплексе». Утверждено Советом Директоров ОАО «Россети» Протокол № 138 от 23.10.2013 г.
6. Официальный сайт АО «МЦСТ» (http://www.mcst.ru).
7. Официальный сайт ОАО «НИПОМ» (http://www.nipom.ru/media/news/nipom-innovatsionnye-resheniya-na-glavnoi-energeticheskoi-vystavke-goda).