Кибербезопасность систем управления современных объектов электроэнергетики - драйвер или тормоз в развитии

Гуревич Алексей

Член ЦК «Кибербезопасность» НТИ EnergyNet
Член исследовательского комитета B5 CIGRE
Индивидуальный член CIGRE

EnergyNet

Центр компетенций **«КИБЕРБЕЗОПАСНОСТЬ»**

Промышленные атаки, какие выводы стоит делать в электроэнергетики?

Яркие примеры последних лет:

- взлом онлайн-платформы для тестирования ПО Codecov, пострадали Rapid7, разработчики софта из компании Hashicorp, облачный провайдер Confluent и сервис голосовых вызовов Twilio (то, что есть в открытых источниках, однако высока вероятность того, что в следствии взлома пострадало гораздо больше компаний);
- масштабная атака шифровальщика REvil (Sodinokibi) на поставщика MSP – решений Kaseya, в результате пострадали по разным оценкам от 1000 до 1500 компаний, пользующихся MSP сервисами, организованными на серверах компании, включая сеть супермаркетов Coop в Швеции, детские сады в Новой Зеландии и некоторые административные учреждения в Румынии,
- масштабная атак на цепочку поставок, ставшая наиболее крупной в истории, на поставщика сервисов по информационной безопасности – SolarWinds, в результате заражения платформы Orion злоумышленники потенциально получили доступ к данным примерно 18 000 клиентов. В результате этого инцидента пострадали Microsoft, Cisco, FireEye, а также множество правительственных агентств США.

Атаки на цепочки поставки приводят к потребности в совместной проработке вопросов кибербезопасности со стороны заказчика и вендоров. Примером синергии может служить следующий подход:

- Распоряжение ПАО «Россети» от 30.05.2017 № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети».
- Приказ ПАО «Россети» от 28.08.2020 № 391, «Методика проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе»

+ выстроенная система аттестации в рамках которой при новом строительстве и реконструкции электросетевых объектов ПАО «Россети» применяется рекомендованное по результатам аттестации оборудование, технологии, материалы и системы. (https://www.rosseti.ru/investment/science/attestation/)

Промышленные атаки, какие выводы стоит делать в электроэнергетики?

Яркие примеры последних лет:

- Атаки на энергосистему Украины: «Прикарпатьеоблэнерго» а также еще 2 энергетических предприятия были атакованы в 2015 году, 230 000 жителей остались без электричества. Также хакеры отключили резервные источники питания, лишив света самих диспетчеров в двух из трёх ЦУС. После отключения мощности на подстанциях хакеры заменили прошивку на установленных там конвертерах serial-to-Ethernet. По завершении операции они запустили зловред под названием KillDisk, чтобы стереть файлы и MBR на компьютерах в центрах управления.

Такие злонамеренные действия породили большую активность со стороны профессионального сообщества не только в области информационной безопасности. В частности в рамках СИГРЭ существует несколько типов рабочих групп (национальные и международные), которые работают в различных исследовательских комитетах.

- ПРГ-2 B5.2/D2 «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»
- D2. РГ4 «Обеспечение информационной безопасности (ИБ) для систем связи и управления в электроэнергетике» (D2.31 Security architecture principles for digital systems in Electric Power Utilities, D2.46 Application and management of cyber security measures for Protection & Control systems).
- WG D2.51_Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System.
- WG B5.66 «Cyber Security requirements for PACS and the Resilience of PAC Architectures».

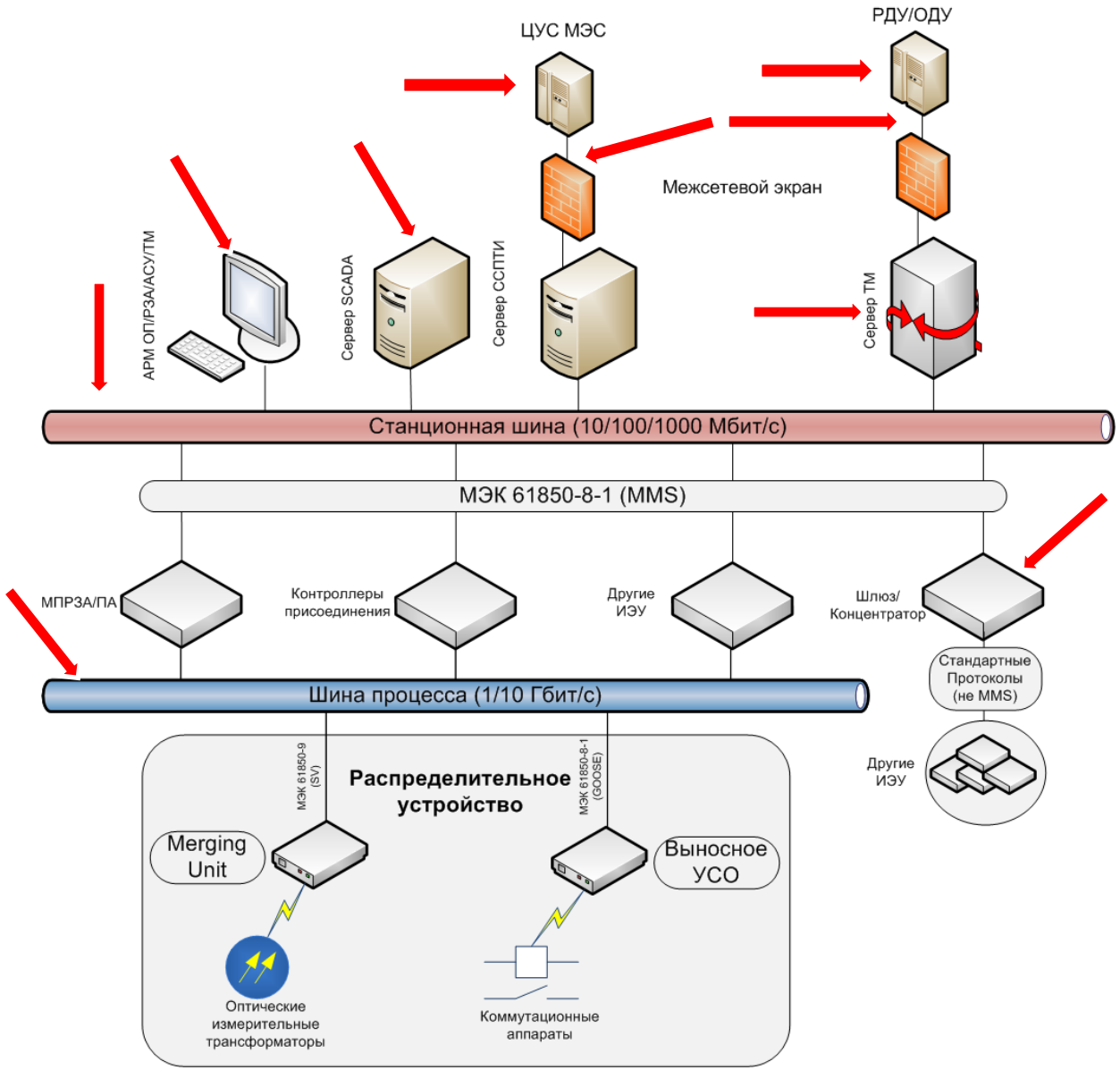
Защищенность современных объектов электроэнергетики

Рассматривая упрощенную схему ЦПС с точки зрения ИБ сразу выделяются следующие узкие места:

- канал с удалённым объектом (ЦУС, ДЦ);
- рабочие станции (АРМ РЗА) и сервера к которым есть доступ внешнего персонала (например, оперативно-ремонтный и персонал сервисных организаций);
- Станционная шина, построенная на физически единых устройствах.

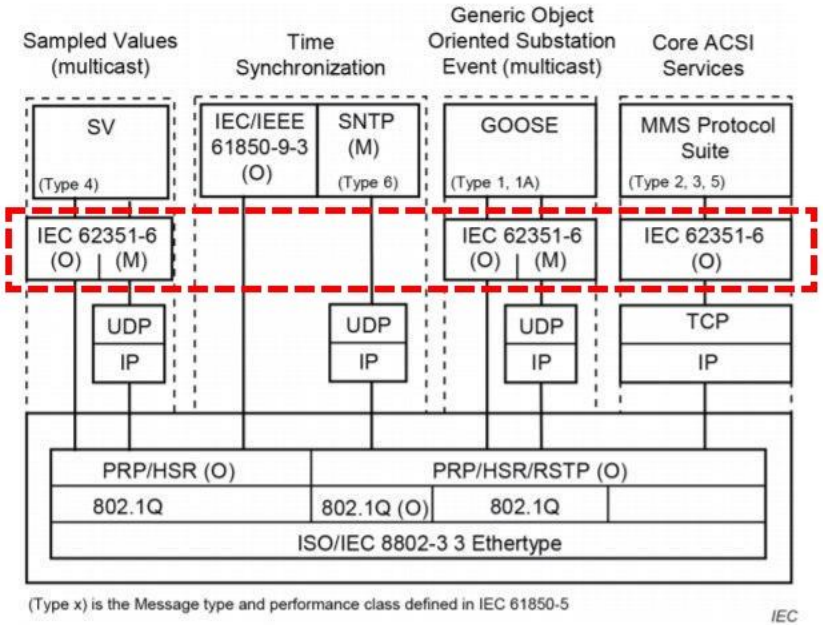
В качестве возможных технологических последствий:

- подмена информации об измерениях параметров режима энергосистемы;
- подача ложных сигналов для терминалов РЗА и АСУ ТП;
- ложные сигналы управления коммутационными аппаратами.



Перевод объектов на протоколы базе стека TCP/IP

Переход от проприетарных протоколов и интерфейсов (RS485, IEC60870-5-101, IEC60870-5-103, ModBus и т. д.) на современные высокоскоростные сети передачи данных (Ethernet, IEC61850). С точки зрения информационной безопасности IEC61850 лучше всего структурирован в IEC 62351, который представляет собой серию стандартов, регламентирующих вопросы безопасности для профилей протоколов на базе стека TCP/IP, в том числе для протоколов IEC 60870-5, IEC 60870-6, IEC 61850.



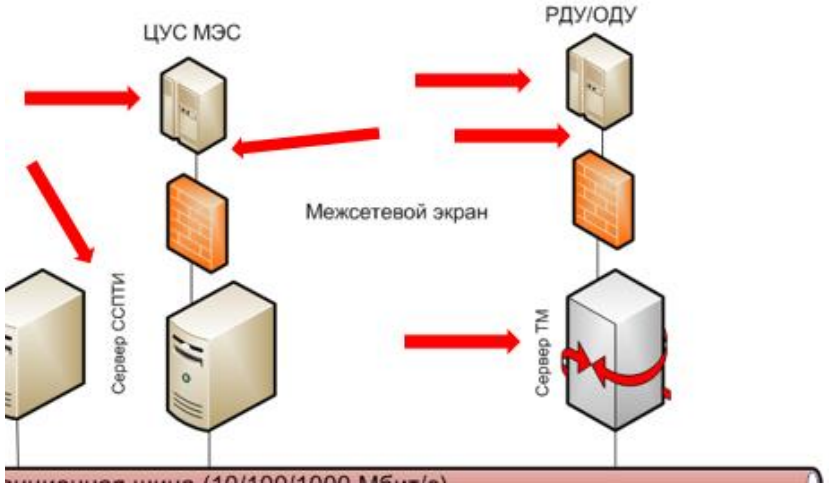
Обсуждаются изменения в обновлённую редакцию стандарта IEC 61850 , где появился IEC 62351-6 «Управление энергетическими системами и связанным с этим обменом информацией. Безопасность данных и коммуникаций. Часть 6. Безопасность для IEC 61850». Для потоков данных, выходящих за пределы ПС, применение IEC 62351-6 будет обязательным.

Перевод объектов на протоколы базе стека TCP/IP

Системный оператор в рамках ТК 016 «Электроэнергетика» инициировал утверждение серии национальных стандартов по цифровому дистанционному управлению ГОСТ Р «Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление в электроэнергетике. Дистанционное управление». *

Среди разрабатываемых требований в виде отдельных ГОСТ анонсирована разработка ГОСТ Р «Реализация защищенного профиля протокола МЭК 60870-5-104 для организации информационного обмена в электроэнергетике Российской Федерации».

Лучшими практиками для защиты передаваемой телеметрии являются методы криптографической защиты информации, описанными в стандартах IEC (МЭК) 60870-5-7, IEC (МЭК) 62351 в части протокола МЭК 60870-5-104.



*https://www.so-ups.ru/news/press-release/press-release-view/news/14110/

А что же вендоры энергетического оборудования?

Примером реализации такой синергии являются поставляемы компанией АО «НИПОМ» терминалы РЗА в периметр ПАО «Россети». При реализации кибербезопасных решений для кроссплатформенной РЗА аппаратная составляющая строится на серийно выпускаемой промышленной вычислительной базе как импортного (Intel, AMD, ARM), так и отечественного (Эльбрус, Байкал) производства, и кроссплатформенном функциональном программном обеспечении ИЭУ, не зависящем от конкретного микропроцессора и операционной системы.*

При этом требования по информационной безопасности (ИБ) изначально закладываются в информационную модель МЭК 61850 ИЭУ, которые имеют следующие встроенные механизмы защиты:

- SSL/TLS-шифрование для MMS между ИЭУ шины процесса и АСУ ТП (SCADA) ЦПС (включая АРМ эксплуатационного и оперативного персонала), а также между ЦУС;
- 2FA на ИЭУ РЗА и АРМ технологической вычислительной сети ЦПС;
- ролевой доступ к элементам интерфейса ИЭУ;
- протоколирование событий безопасности на уровне отдельного ИЭУ, ЦПС и ЦУС.

* https://www.fsk-ees.ru/press_center/company_news/?ELEMENT_ID=340932

Импортозамещение

Постановление Правительство РФ 28.08.2021 (№1432).
В Госзакупках вводится запрет в отношении импортных интегральных микросхем, смарт-карт, ноутбуков, планшетов, компьютеров, серверов и светотехнической продукции.

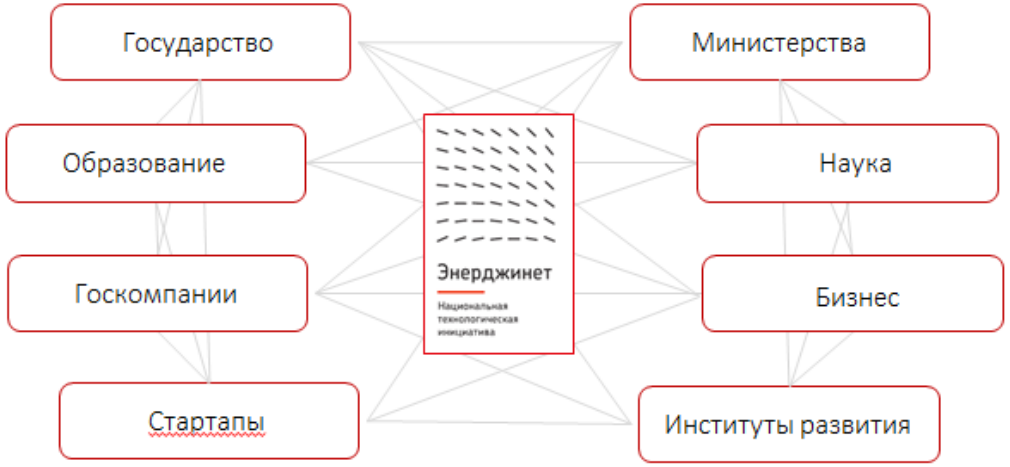
Приказ Министерства промышленности и торговли РФ 02.08.2021 N 2915
План мероприятий по импортозамещению в социально значимых отраслях промышленности Российской Федерации на период до 2024 года

Проект по поручению Правительства, разработанный Минцифры по вопросам внедрения госкомпаниями российской радиоэлектроники в сквозные проекты, которые направлены на возможность комплексно развивать электронику в плотном взаимодействии заказчиков, разработчиков программного обеспечения и аппаратного оборудования.

Другой важнейший аспект – локализация производства, то есть, снижение зависимости от иностранных поставщиков.

Energynet — точка сборки национальных инициатив в области создания интеллектуальной электроэнергетической систем.

Energynet — точка сборки национальных инициатив в области создания интеллектуальной электроэнергетической систем.



Центры компетенций НТИ

Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем

Автономная энергетика

Технологии новых и мобильных источников энергии

Интеллектуальная распределенная энергетика

Стандартизация и оценка соответствия

Экспертно-аналитический центр «Энерджинет»

Кибербезопасность НТИ «Энерджинет»

Архитектурный комитет

Группа НПА

Рабочая группа

Экспертная деятельность ЦК «Кибербезопасность» НТИ ЭнерджиНЕТ

В рамках работы эксперты Центра компетенций по кибербезопасности в электроэнергетике НТИ EnergyNet приняли участие в 2019 году в разработке следующих документов:

a. Методические рекомендации по определению и категорированию ОКИИ ТЭК, согласованные Министерством энергетики и ФСТЭК России (https://minenergo.gov.ru/view-pdf/11357/102517).

b. Аналитический отчет «Кибербезопасность в электроэнергетике», опубликованный на сайте НТИ EnergyNet в феврале 2020 (https://energynet.ru/upload/Кибербезопасность%20в%20электроэнергетике.pdf).

c. Аналитический отчет «Об импортозамещении в электроэнергетике России», сформированный на основе анализа опроса участников VI международной научно-практической конференции «Цифровая трансформация в электроэнергетике» и выставке «релавэкспо-2021» (Чебоксары, апрель 2021)

Energynet

Национальная технологическая инициатива

Экспертная деятельность ЦК «Кибербезопасность» НТИ ЭнерджиНЕТ

Отечественная электронная компонентная база (ЭКБ)
63.6 % положительно относятся к импортозамещению.
При этом 54,5 % опрошенных имеют представление об отечественной ЭКБ, а 18,2 %. применяет в разработках отечественную ЭКБ

Отечественное программное обеспечение (ПО)
90% опрошенных имеют представление об отечественном ПО
59,1% применяют отечественное ПО в своих разработках.

54,5 % опрошенных производителей ПО и ЭКБ занимаются включением своей продукции в Единый реестр российских программ для электронных вычислительных машин и баз данных и Единый реестр российской радиоэлектронной продукции

Выполнение требований информационной безопасности

Более 70 % опрошенных компаний обеспечивают соответствие своей продукции требованиям информационной безопасности (ИБ) независимо от наличия требований заказчиков продукции.

Менее **25%** опрошенных компаний готовы инвестировать ресурсы в стандартизацию ИБ своей продукции.
Менее чем у **14 %** компаний процессы обеспечения ИБ находятся на высоких уровнях зрелости.

Energynet
Национальная технологическая инициатива

Кибербезопасность драйвер или тормоз?

Производители видят две основные проблемы импортозамещения:

- достаточно трудно обеспечить полную цепочку производственного цикла за счет исключительно российской электронной компонентной базы;
- не все участники рынка уделяют достаточно внимания решению проблем информационной безопасности, что в условиях как реальных угроз, так и требований нормативных документов снижает привлекательность применения оборудования с интегрированным ИБ-функционалом.

С практической точки зрения целесообразно для повышения защищенности:

- рассматривать гармонизацию серий стандартов IEC 62351 и IEC 62443 для использования в рамках процессов обсечения информ. безопасности создаваемого ПО и оборудования в РФ;
- развивать персональные компетенций по вопросам кибербезопасности;
- вендорам энергетического оборудования необходимо использовать комплексный подход в обеспечении кибербезопасности поставляемых продуктов и систем, выражающийся в реализации концепции secure-be-design, подготовке комплексных решений, учитывающих все лучшие мировые практики по обеспечению кибербезопасности, созданию и развитию сервисов в данной области.

Спасибо за внимание!

Гуревич Алексей
alexeyg09@gmail.com

EnergyNet
Центр компетенций **«КИБЕРБЕЗОПАСНОСТЬ»**

cigré