Российский национальный комитет Международного Совета
по большим электрическим системам высокого напряжения

ФГБОУ ВПО «Ивановский государственный энергетический
университет имени В.И. Ленина»

ПИСЬМЕННЫЙ ПЕРЕВОД

научно-технического теста для участия в конкурсе переводчиков научно-технической литературы Молодежной секции РНК СИГРЭ

Выполнили: студенты

Гудухина А.А. – С.5-21
Шляцкая Е.М. – С.21-37
Профьев М.В. – С.37-47
Грибанова Т.А. – С.48-54
Матисова К.М. – С.54-66
Назарова П.Н. – С.66-82
Володина Ю.С. – С.82-96

Редактор: Гудухина А.А.

Иваново 2016

Принципы архитектурной безопасности цифровых систем энергетических компаний

Рабочая группа

D2.31

Апрель 2015

Участники

Дженс Зербст (Jens Zerbst) (Организатор), Лудовик Пйетрэ-Комбэсэдэс (Ludovic Piètre-Cambacédès) (Организатор[1]), Матиас Екстед (Mathias Ekstedt) (Секретарь), Джованна Дондосола (Giovanna Dondossola), Кристоф Пойриер (Christophe Poirier), Паскаль Ситбон (Pascal Sitbon), Эйдж Торкилсен (Åge Torkilseng), Деннис Хольстайн (Dennis Holstein), Джон Макдональд (John McDonald), Роберт Иванс (Robert Evans), Марк Тричлер (Marc Tritschler), Симон Циммерман (Simon Zimmermann), Лиро Ринта Жуппи (Liro Rinta Jouppi), Горан Эрикссон (Göran Ericsson), Марк Шерер (Marc Scherer), Февен Зегаи (Feven Zegai), Оливиер Бретон (Olivier Breton)

В память о Торе Алборге

ISBN: 978-2-85873-317-0

---

[1] 2010 - 2012

Содержание

1 Введение

До начала цифровой эры электроэнергетические компании не видели угрозы со стороны сети Интернет. Они полагались на секретность своих систем и физическую защиту. Эти системы соединялись не протоколами передачи данных, а реле и физическими коммутаторами.

Сегодня производство, передача и распределение электроэнергии все больше зависят от цифровых систем, в том числе от Промышленной Автоматизации и Систем Управления, информационных систем, коммуникационных сетей, например:

- Электроэнергетические компании все больше контролируют производство, распределение и передачу энергии, и при этом централизованно используют цифровые системы вместо локального, децентрализованного управления. В мире, где компании стремятся к сокращению расходов и совершенствованию управления, внедрение цифровых систем необратимо, поскольку они не могут позволить себе возвращение к ручному труду.

- Растущее число возобновляемых источников энергии влияет на работу сетей электроснабжения и делает ее более требовательной к автоматизированному контролю и, таким образом, управление ими становится невозможным без цифровых систем.

- Умные сети электроснабжения и их многочисленные новые службы будут полагаться на распределенную автоматизацию и новые требования к клиентам, и, следовательно, коренным образом изменят схемы доступа к сети, базовую архитектуру и использование цифровых систем. [1-1]

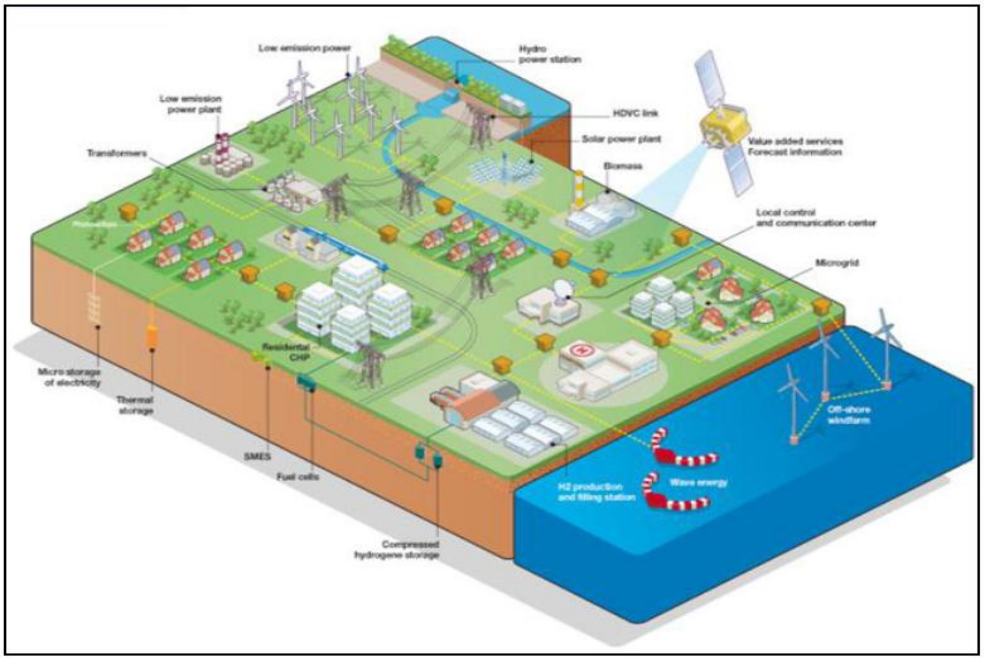

Рисунок 1-1 Схема «Умной сети» Европа компании Electricite de France [1-2]

Настоящий отчет является результатом работы рабочей группы D2.31, целью которой являлось обсуждение и разработка «Принципов архитектурной безопасности цифровых систем энергетических компаний» по следующим ключевым направлениям:

- Классификация методов определения зон / уровней безопасности, связанных с дифференцированным подходом к безопасности
- Характеристика, классификация и моделирование угроз
- Удаленное обслуживание

1.1 Опасность цифровых систем

Эволюция цифровых систем и зависимость от них базовых процессов электроэнергетических компаний уменьшили надежность электроснабжения, так как внедряют уязвимости в цифровые системы, архитектуру и коммуникации.

1.1.1 Изменение технологий

Электроэнергетические компании привыкли к длительным срокам службы их технической инфраструктуры. Патентованные системы были нормой; они были спроектированы и построены специально в индивидуальных целях. За последнее десятилетие развитие технологий и характер бизнеса изменились. Современное оборудование построено из

готовых модулей коммерческого исполнения, стандартного аппаратного и программного обеспечения, которое предназначено для производственных и других целей. В целом промышленность перешла от конкретного оборудования и программного обеспечения к универсальным операционным системам и стандартным приложениям, которые могут использоваться и для различных целей. Аналогичное развитие получают человеко-машинный интерфейс (ЧМИ), программируемые логические контроллеры (ПЛК), а также других средства защиты и автоматизации оборудования. Сегодня цифровые системы с одной и той же операционной системой и с одинаковыми уязвимостями могут использоваться и в офисной среде, и в системах диспетчерского управления и сбора данных, и на подстанциях для подключения к реле защиты.

То же самое верно и для обмена данными. Передача данных при осуществлении управления и работе базовых процессов электроэнергетических компаний раньше имела вид "последовательной линии передачи" и соединения "точка-точка". Сегодня обмен данными в таких компаниях базируется на современных "маршрутизируемых" коммуникационных протоколах (например, на IP-протоколах), которые вводят новый уровень связи с новыми уязвимостями. Возвращение к старым последовательным протоколам не даст достичь пропускной способности, необходимой для запуска современных приложений, таких как мониторинг глобальной территории, и не предоставит столько же возможностей, сколько дают IP-протоколы.

1.1.2 Увеличение взаимосвязанности систем

Статья в немецкой газете [1-3] [1-4] описывает реальный пример, который продемонстрировал укрепление связи между коммерческими сетями и цифровыми системами контроля за потенциально опасными объектами жизнеобеспечения в реальном мире. В статье описывается эксперимент, в ходе которого была предпринята попытка проникновения в электроэнергетическую компанию, расположенную в Германии и поставляющую электричество и воду примерно 40 000 жителей региона. Согласно статье, специалист в сфере информационной безопасности за короткий срок может получить доступ к цифровым системам контроля опасного объекта жизнеобеспечения через коммерческую или бизнес-сеть используя их уязвимости, а также при помощи комбинаций таких методов атак, как социальная инженерия.

Несмотря на то, что это касается не всех электроэнергетических компаний, их инфраструктур и уровней безопасности, становится ясно, что полная изоляция систем

управления от бизнес-систем - это миф [1-5]. Этот миф уже достаточно давно не позволяет компаниям принять адаптированное кибербезопасное положение.

В качестве еще одного примера того, как используется подключение к системам, можно изучить упрощенную архитектуру завода, показывающую различные направления атак вредоносной программы "Stuxnet" [1-6].

Производственные и бизнес IT-системы уже сегодня подключены к цифровым системам потенциально опасных объектов жизнеобеспечения.

Увеличение числа коммуникаций и интеграция - это направления развития электроэнергетических компаний, которые уже не остановить. Они выражаются в более широком использовании удаленного доступа, функциональной совместимости открытых коммуникаций и стандартных моделей данных, таких как МЭК 61850 [1-7]. Чем больше растут взаимосвязанность и интеграция, тем больше электроэнергетических компаний подвергается кибератакам с потенциально значимыми последствиями.

Новые требования рынка демонстрируют необходимость подобных связей, электронного обмена данными, интеграции и т.п.:

- Поддержка 24/7 в сочетании с ценовым давлением требует использования удаленных служб, которые должны быть доступны по всему миру и иметь повышенную пропускную способность для удовлетворения новых требований, диктуемых постоянно растущими темпами передачи и размерами пакетов услуг, обновлений и конфигураций.

- Энергетическая отрасль уходит от управления спросом на ценозависимое потребление, что позволяет производителям энергии и клиентам взаимодействовать в автоматизированном режиме в реальном времени, тем самым координируя спрос, чтобы сгладить пики потребления. Двунаправленные потоки энергии для распределенной генерации также требуют новых коммуникаций. Все это значительно увеличивает количество рыночных агентов и необходимых коммуникаций.

- Энергетическая система должна включать в себя больше возобновляемых источников энергии, которые по своей природе менее управляемы, чем ее традиционная выработка. Это должно быть компенсировано более высокой

степенью взаимосвязанности и интеграции.

- Умное измерение значительно расширяет коммуникационные потребности по сравнению с тем, что было раньше, и предоставляет возможность контроля в помещениях клиентов. И по мере того, как растет взаимосвязанность систем, их критичность повышается теми же темпами. Неожиданно, вся энергетическая система оказалась в зависимости от надежности коммуникаций. Без нее существует риск масштабных отключений электроэнергии [1-8].

Даже если системы становятся все сложнее и создают новые направления для атак, мы по-прежнему должны помнить об устаревающих системах. В октябрьской статье 2013 года [1-9], исследователи сообщили о чувствительности к атакам некоторых элементов в устройствах, которые используются в последовательных и сетевых коммуникациях между серверами и подстанциями. Эти устройства часто игнорировались как объекты, подверженные риску со стороны хакерских атак, потому что безопасность энергетических систем была сосредоточена только на IP-протоколах, а последовательные линии связи не считались важными или жизнеспособными направлениями для атак (см. [1-5]). Однако исследователи говорят, что нарушение системы питания через последовательные устройства связи может быть на самом деле проще, чем атаки через IP-сети, так как это не требует обхода брандмауэров. Нарушение безопасности также возможно при более поздней интеграции в существующие последовательные устройства [1-10] интерфейсов IP-сетей, поддерживающих функции удаленного технического обслуживания.

1.1.3 Рост числа угроз

Согласно недавнему отчету команды быстрого реагирования на кибератаки промышленных систем управления (ICS-CERT) [1-11], энергетика - это кибермишень в промышленном секторе. Кроме того, поставщик антивирусного программного обеспечения подтверждает рост числа угроз в отчете, опубликованном в начале 2014 года, где говорится, что "энергетический сектор стал одним из основных направлений для целенаправленных атак и в настоящее время входит в пятерку целевых секторов по всему миру" [1-12].

Увеличение числа угроз отражается и на техническом уровне. Число отчетов об уязвимости систем диспетчерского управления и сбора данных выросло на 600% по сравнению с 2010 г., при этом в период с 2011 по 2012 год количество обнаруженных

уязвимостей удвоилось [1-13]. Эти цифры свидетельствуют об увеличении интереса со стороны хакеров, принимая во внимание тот факт, что для некоторых операторов стало обязательным составление отчетов об инцидентах. Эти уязвимости обнаруживаются в широком спектре устройств и производителей, а их количество превышает число уязвимостей в технологиях Java или Flash. Это является существенным фактором, так как эти технологии часто рассматривают как программное обеспечение с низким уровнем безопасности [1-13].

Чтобы нарисовать более дифференцированную картину современных угроз[2] для цифровых систем электроэнергетических компаний, их можно разделить на направленные и ненаправленные атаки [1-14].

Примеры направленных атак:

- Хорошо финансируемые государством или организациями атаки, в которых предпочитают использовать вредоносное программное обеспечение "Stuxnet" [1-15], которое, вполне вероятно, разрушило иранскую ядерную программу, или "Dragonfly Group", которое способно создать угрозу диверсии против западных энергетических компаний [1-16].
- Атаки хакеров с политическими или экологическими задачами. Такими активистами являются "Anonymous". Их целями являются энергетические компании, такие как ядерные EDF, GE и ENEL в Q2 / 2011 после трагедии на Фукусиме [1-17]. К подобным атакам можно отнести "Shamoon virus attack"[3], в ходе которой было заражено около 30000 компьютеров в нефтяной компании в Саудовской Аравии в 2012 году [1-18].
- Особое беспокойство вызывают недовольные работники, вспомогательный персонал, третьи лица с утвержденными правами доступа и знаниями тонкостей эксплуатации электроэнергетических установок и хранилищ, содержащих конфиденциальные данные [1-19].

Примеры ненаправленных атак:

---

[2]Картина не является исчерпывающей: Дальнейшая дифференциация, например, на преднамеренные и не преднамеренные угрозы не закончена

[3]После публикации на Pastebin.com появилось мнение, что атака "Shamoon virus attack" была организована группой хакеров.

- Тестирование собственных возможностей и технологий: например, попытки найти соединенные с Интернетом системы диспетчерского управления и сбора данных с известными уязвимостями с помощью поисковой системы "Shodan computer search engine" [1-20]
- Вредоносные вирусы: например, "Slammer worm" воздействующий на американскую атомную электростанцию в Огайо [1-21] во время ее обслуживания.

Не все из перечисленных атак требуют сложных инструментов или серьезного финансирования, но в целом они становятся все более сложными, с более изощренной тактикой и значительными возможностями.

Из всего вышесказанного можно заключить, что с развитием инфраструктуры интеллектуального учета Умных сетей электроснабжения изысканность и интенсивность подобных угроз будет только расти. Ситуация усугубляется, когда инфраструктура подключена к сети Интернет общего пользования и не защищена от угроз путем использования корпоративных или частных внутренних сетей или выделенных систем.

Электроэнергетические компании должны внимательно следить за быстро эволюционирующими угрозами и защищать соответствующим образом конфиденциальную информацию и цифровые системы.

1.2 Современная помощь, доступная электроэнергетическим компаниям

Текущая ситуация не изменится без новых требований к безопасности для цифровых систем и базовых архитектур, используемых в электроэнергетических компаниях. Эти требования к безопасности должны быть получены при надлежащих оценках рисков и общих архитектурных решений.

Термин "кибербезопасность", используемый в данном контексте, определяется следующим образом:

"Кибербезопасность стремится сохранить доступность и целостность сетей и инфраструктуры, а также конфиденциальность информации, содержащейся в них." [1-22]
Кибербезопасность в первую очередь касается людей, процессов и технологий, работающих вместе "чтобы охватить весь диапазон сокращения числа угроз, уменьшения уязвимости, сдерживания, международного взаимодействия, реагирования на инциденты, отказоустойчивости, а также политики и мероприятий по восстановлению, в том числе сетевые компьютерные операции, защита информации, обеспечение правопорядка и т.п." [1-23]

1.2.1 Современное развитие в области стандартизации

Растущее осознание кибер-рисков подтолкнуло электроэнергетические компании исследовать стандарты безопасности, применяемые в настоящее время для цифровых систем [1-24]. В последнее время комитеты по стандартизации начали анализ стандартов связи и безопасности, примеряя их на «Умные сети».

Американский Национальный институт стандартов и технологий (НИСТ) создал комплексное руководство, содержащее анализ уровней риска, требования безопасности и оценки основных логических сетевых интерфейсов [1-25]. В 2013 году 15-ая рабочая группа 57-ого технического комитета Международной Электротехнической Комиссии (МЭК) опубликовала сборник литературы по кибербезопасности «Умных сетей» [1-26]. Объединенная рабочая группа Европейского комитета по стандартизации (ЕКС), Европейского комитета по электротехническим стандартам (ЕКЭС) и Европейского института стандартов связи (ЕИСС) по вопросам стандартизации «Умных сетей» приступила к анализу стандартов путем сопоставления их с доменами и зонами контроля основных приложений «Умных сетей» [1-27].

- Что касается поддержки, оказываемой электроэнергетическим компаниям, внимания заслуживают три характерные инфраструктуры защиты, которые осуществляют всестороннее управление безопасностью. Комитет перерабатывающей промышленности ISA99, принимает достаточно активное участие в разработке спецификаций, ориентированных на процессы и продукцию, которые могут применяться как в данной отрасли, так и в энергетике. Их передовые проекты используются в качестве базы в МЭК (в 65-ом техническом комитете), и в последствии превращаются в стандарты МЭК или технические отчеты (серии МЭК 62443) за исключением таких, как МЭК 62443-2-4, который базируется на WIB документах [1-28].
- Технический отчет 27019 международной организации по стандартизации (ИСО) и МЭК дополняет набор элементов управления, содержащихся в стандарте ИСО / МЭК 27002, и содержит дополнительные указания по осуществлению контроля в соответствии со специфическими требованиями энергетической отрасли.
- Особого внимания со стороны электроэнергетических компаний заслуживает инфраструктура кибербезопасности, недавно выпущенная НИСТ [1-29], которая создана, чтобы помочь операторам потенциально опасных объектов жизнеобеспечения улучшить их кибербезопасность.

Поставщики систем управления также принимают активное участие в разработке и внедрении технологий безопасности, связанных со стандартными протоколами связи, такими, как серия МЭК 61351 находящаяся в ведении 15-ой рабочей группы 57-ого технического комитета МЭК. Кроме того, область ядерной электроэнергетики имеет собственные программы и инициативы на национальном (например, план кибербезопасности института ядерной энергетики (NEI) 08-09 в США [1-30]) и на международном уровнях (документ МАГАТЭ [1-31] и стандарты МЭК, такие как МЭК 62645 или МЭК 62859 [1-32]).

1.2.2 Инициативы государств и организаций

Широкое распространение «Умных сетей» электроснабжения побудило страны ЕС и США создать более комплексные программы внедрения. Они разработали и поддерживают стратегический план энергетического сектора для достижения кибербезопасности систем доставки электроэнергии.

Верховный представитель ЕС по внешней политике и безопасности изложил видение ЕС и обозначил действия, необходимые для получения открытого, безопасного и надежного киберпространства для своих государств-членов [1-33].

Это видение сформулировано в пяти стратегических приоритетах:

1. Достижение киберустойчивости
2. Значительное уменьшение киберпреступности
3. Разработка политики кибероборонь и возможностей, связанных с Общей политикой безопасности и обороны (ОПБО)
4. Разработка промышленных и технологических ресурсов для кибербезопасности
5. Установка согласованной международной политики касательно киберпространства для ЕС и продвижение основных ценностей ЕС.

Реализация этой стратегии началась в конце 2013 года и получила развитие в 2014 году. Европейское агентство по сетевой и информационной безопасности (ЕАСИБ) было создано в 2004 году и в настоящее время Совет ЕС и Парламент обсуждают новые положения по его укреплению и модернизации. Совместно с другими учреждениями ЕАСИБ играет ключевую роль во внедрении и распространении данной стратегии.

Например, комиссия обратилась к ЕАСИБ по следующим вопросам:

- Оказание помощи государствам-членам ЕС в разработке возможностей в области национальной киберустойчивости, в частности, путем представления заключений по вопросам безопасности и устойчивости промышленных систем управления, транспорта и энергетической инфраструктуры.
- Разработка технических руководств и рекомендаций для принятия стандартов сетевой информационной безопасности (СИБ) и передового опыта в государственном и частном секторах в сотрудничестве с соответствующими национальными компетентными органами, заинтересованными сторонами, европейскими и международными органами по стандартизации, а также с Объединенным исследовательским центром (ОИЦ) Европейской комиссии.
- Выявление новых тенденций и потребностей ввиду эволюции киберпреступности и моделей кибербезопасности для того, чтобы разрабатывать отвечающие требованиям цифровые инструменты и технологии.

Для того чтобы облегчить и поддержать процесс внедрения «Умных сетей» электроснабжения по всей Европе, Европейская комиссия создала целевую группу по «Умным сетям». Целью данной рабочей программы является выявление и подготовка ряда нормативных рекомендаций для обеспечения согласованного и быстрого внедрения «Умных сетей» по всей Европе, в результате чего все участники получат ожидаемые выгоды. Ключевым результатом работы второй экспертной группы является определение надлежащего нормативного плана и рекомендаций по обработке данных, их безопасности и защиты. Ее цель - заложение основ конфиденциальности данных и инфраструктуры защиты, которая призвана как охранять информацию, так и предоставлять доступ к ней. Исходя из результатов программы второй экспертной группы, ЕАСИБ недавно предложил перечень мер безопасности для «Умных сетей» электроснабжения [1-34]. Этот список используется как основополагающий в рабочей группе по информационной защите, которая является частью координационной группы ЕКС, ЕКЭС и ЕИСС по вопросам стандартизации «Умных сетей», для сопоставления стандартов безопасности и определения необходимости дальнейшей разработки неудовлетворенных требований. Европейский проект по безопасности энергетических систем находится на шаг впереди в отношении ликвидации брешей, обнаруженных экспертными группами [1-35].

Начиная с 2005 года Министерство энергетики США в сотрудничестве с другими агентствами США и Канады способствовали развитию стратегических планов по обеспечению безопасности систем управления в энергетическом секторе с целью

повышения кибербезопасности во всей энергетической отрасли. В 2011 году был обновлен стратегический план [1-36], который включил изменения в технологиях «Умных сетей», которые разработаны на основе новых приоритетов. Эти приоритеты включают тенденции к ускорению раскрытия уязвимостей, которые являются результатом появления более современных угроз. Особое внимание обращается на культуру безопасности, которая выходит за рамки простого соответствия. Цель США - к 2020 году разработать устойчивые системы поставки энергии, которые будут строиться, устанавливаться, эксплуатироваться и обслуживаться таким образом, чтобы пережить кибератаки, сохранив при этом критически важные функции.

1.2.3 Роль СИГРЭ

СИГРЭ оказывала поддержку электроэнергетическим компаниям в решении вопросов по кибербезопасности. В этом разделе представлены рабочие группы научного комитета СИГРЭ, связанные с темой кибербезопасности:

Объединенная рабочая группа (ОРГ) СИГРЭ D2/B3/C2-01, “Безопасность информационных систем и внутренних сетей Интранет в электроэнергетических системах”. Она существовала с 2003 по 2006 год. ОРГ выпустила техническую брошюру [1-37], цель которой заключалась в повышении осведомленности о кибербезопасности в электроэнергетических системах, а также предоставлении некоторых рекомендаций по решению проблем с безопасностью путем сосредоточения внимания на моделировании защищаемой зоны, методах оценки рисков, и создании инфраструктуры защиты.

Рабочая группа СИГРЭ D2.22, "Анализ информационной безопасности в электроэнергетических компаниях". Она существовала с 2006 по 2009 год как продолжение работы ОРГ D2/B3/C2-01. Рабочая группа D2.22 углубилась в исследование следующих вопросов: базовые принципы управления информационной безопасностью для электроэнергетических компаний; оценки рисков, базовые модели и методы предотвращения появления уязвимостей, угроз и нападений; и технологии безопасности для систем диспетчерского управления и сбора данных, включая сети управления в режиме реального времени [1-38].

СИГРЭ D2.38 “Базовые принципы действий для операторов потенциально опасных инфраструктур в электроэнергетических компаниях в ответ на киберугрозы. После выпуска в 2015 году техническая брошюра этой группы включает базовые принципы

использования набора инструментов, который операторы электроэнергетических установок смогут использовать для автоматизации реагирования на киберугрозы. Конкретные компоненты набора инструментальных средств будут отбираться на основе данных, полученных из опроса электроэнергетических компаний, заинтересованных в данном наборе инструментов для автоматизации ответов на кибератаки.

СИГРЭ B5-D2.46 "Применение и управление мерами кибербезопасности для систем защиты и управления". Создание технической брошюры в этой группе близится к завершению, и основное внимание в ней уделяется вопросам кибербезопасности с точки зрения систем защиты и управления, в том числе обсуждению угроз, справочной информации, стандартов, практическим решениям и конкретным исследованиям.

2 Рабочая группа D2.31

Рабочая группа D2.31 была сформирована в качестве преемницы Рабочей группы D2.22. Ее цель - разработка принципов работы архитектуры безопасности для цифровых систем, использующихся в электроэнергетических компаниях. Масштабы работы включают обсуждение общих принципов архитектуры безопасности для цифровых систем, изучение некоторых аспектов и решение конкретных вопросов. Рабочая группа существовала с 2010 по 2014 год.

Она разделила свою деятельность на три рабочих направления:

- Первое рабочее направление: Классификация методов для определения зон и уровней безопасности (дифференцированный подход)
- Второе рабочее направление: Характеристика, классификация и моделирование угроз
- Третье рабочее направление: Удаленное обслуживание

Рабочая группа D2.31 за время службы подготовила следующие публикации и инициировала следующие виды деятельности:

- Статья "Дифференцированный подход к кибербезопасности электроэнергетических компаний: Пояснение уровней безопасности и понятия зон" была представлена на коллоквиуме D2 в 2011 году в Буэнос-Айресе. [2-1]
- Статья "Моделирование кибератак для оценки безопасности Умных сетей электроснабжения" была представлена на коллоквиуме D2 в 2011 году в Буэнос-

Айресе. [2-2]

- Статья "Моделирование кибератак и дифференцированный подход к безопасности: ключевые элементы при проектировании архитектуры безопасности на электроэнергетических предприятиях» была представлена на Парижской сессии СИГРЭ в 2012 году. [2-3]
- Статья «На пути к адаптированной методологии для классификации дифференцируемых подходов к безопасности в архитектурах электроэнергетических компаний" была представлена на симпозиуме D2 в 2013 году в Лиссабоне. [2-4]
- Статья "Применение базовых оценок кибербезопасности для архитектур Умных электросетей" была представлена на коллоквиуме D2 в 2013 в Индии. [2-5]
- Рабочая группа представила "Руководство по вопросам кибербезопасности" на Международном коллоквиуме СИГРЭ по теме "Умные сети электроснабжения" в Индии в 2013 году.
- Статья "Безопасность удаленных сервисов, используемых электроэнергетическими компаниями" была отправлена на Парижскую сессию СИГРЭ в 2014 году [2-6]
- Статья "Статус кибербезопасности" была опубликована в журнале Electra в октябре 2014 года. [2-7]

3 Краткое содержание результатов работы и рекомендаций рабочей группы D2.31

Сегодня производство, передача и распределение электроэнергии все больше зависят от цифровых систем, в том числе от информационных систем и коммуникационных сетей. Эта зависимость уменьшает надежность электроснабжения, так как увеличивает количество уязвимых мест в цифровых системах, архитектуры и коммуникации. Именно поэтому появилась необходимость рассмотреть вопрос об угрозах кибербезопасности и рисках для всех организаций, а также повысить осведомленность всех работников, начиная от операторов систем и заканчивая руководством, включая поставщиков, партнеров и сторонних организаций.

В данной области рабочая группа D2.31 завершила свою деятельность, обнародовав

следующие результаты работы.

- Классификация методов для определения зон и уровней безопасности первого рабочего направления (дифференцированный подход):
  - Электроэнергетические компании сталкиваются с новыми проблемами с точки зрения кибербезопасности из-за непрекращающейся эволюции окружения и технической инфраструктуры. Многочисленные стандарты, передовые методы и проектные чертежи добиваются дифференцированного подхода к безопасности, а также создания зон безопасности.
  - Успех дифференцированного подхода к безопасности зависит от эффективности его реализации, обслуживания и эксплуатации. Чтобы облегчить переход к дифференцированному подходу и его соблюдению, необходимы практические методики, руководства, шаблоны и ссылки на стандарты и передовые методы. Эффективная практическая методология ввода дифференцированного подхода к обеспечению безопасности в электроэнергетических компаниях заключается в разработке и реализации классификационного подхода для конкретного бизнеса, технологии или приложения, используемого на производстве.

    В дополнение к ускоренному переходу на дифференцированный подход к проектированию безопасности эта методика может исключить необходимость проверки безопасности, так как она выявляет расположение критических систем, которые требуют специального управления. Для получения более значительных результатов следующим шагом может быть создание общего определения дифференцированного подхода и требований, которые необходимо установить для конкретных областей «Умной сети».

- Характеристика, классификация и моделирование угроз второго рабочего направления:

  Графическое моделирование атак является одновременно актуальным и жизнеспособным методом анализа киберзащищенности архитектур систем управления будущими Умными электросетями. Производится всестороннее моделирование атак, и одним из самых простых подходов к этому процессу является построение «деревьев атак». В результате использования данного несложного подхода получается значение, которое дает первое целостное представление о сильных и слабых сторонах данного архитектурного решения

системы. Подобные модели могут быть расширены в объемах или детализированы, если это необходимо.

Если заглянуть глубже, то моделирование и оценки инструментов, анализирующих безопасность архитектур ИКТ, позволяет управлять сложностью связей между компонентами конфигураций, атаками и контролем безопасности. Исходя из предположения, что конфигурации архитектур являются краеугольным камнем кибербезопасности «Умных сетей», данная работа исследовала применение приложения CySeMoL для анализа безопасности вариантов архитектур регулирования напряжения в активных электросетях, соединяющих распределенные энергоресурсы. Мы представили архитектуру регулирования напряжения используя мета-модель, созданную приложением CySeMoL, и оценили вероятность успешной атаки, сравнив три конфигурации.

В работе также акцентируется внимание на многих проблемах, по сей день возникающих при графическом моделировании атак на электроэнергетические компании. Очевидно, что использование графического моделирования атак в практических приложениях требует ряда компромиссов, начиная с выбора между простыми методами моделирования (например, деревьями) и более сложными вероятностными и динамическими подходами. Кроме того, влияние оказывает и уровень детализации, используемый для описания сценариев работы Умных электросетей. Для получения полной модели необходимо добавить более детализированную информацию о различных компонентах ИКТ системы и о других функциональных возможностях управления при помощи Умной электросети. Кроме того, может возникнуть необходимость в рассмотрении других возможных атак и дополнительных целей, кроме представленных в примере. В дополнение к сказанному, возможно добавление контрмер, если в этом есть необходимость. И, наконец, для того, чтобы графическое моделирование атак стало реальной практической поддержкой для принятия решений в электроэнергетических компаниях, в него необходимо включить анализ последствий атак как для энергетических систем, так и для бизнеса в целом. Многие из этих вопросов остаются открытыми и нуждаются в дальнейшей проработке.

- Третье рабочее направление: Удаленное обслуживание

  Электроэнергетические компании используют удаленный доступ для нескольких целей, например, для технического обслуживания или мониторинга. В то время как повышаются производительность и скорость всего процесса, появляются и новые риски. Во многих случаях удаленный доступ осуществляется сторонними организациями, а несогласованность политики безопасности ведет к ослаблению предприятий.

  В целях оказания поддержки усилиям компаний в этой области, мы предложили упрощенный контрольный список, который применим к удаленным службам. Ожидается, что этот контрольный список поможет понять, нуждается ли предприятие в удаленных службах, предоставляемых сторонними организациями, и какие требования должны быть включены в запрос коммерческого предложения.

  Мы также обсудили возможные технические архитектуры и способы снижения рисков.

  Дальнейшие шаги включают внедрение систем дистанционного обслуживания в устаревшие устройства, обзор различных архитектур для дистанционного обслуживания, их техническое сравнение, а также проблемы, возникающие при использовании мобильных электронных устройств (например, планшетов, смартфонов и т.д.) для осуществления дистанционного обслуживания. Должны быть проанализированы вопросы, связанные с расширением удаленного доступа, включая цели использования дистанционного управления.

4 Первое рабочее направление: Классификация методов для определения зон и уровней безопасности (дифференцированный подход)

Целями первого рабочего направления являются обсуждение и разработка:

- общего обзора известных стандартов, передовых методов и проектных чертежей
- общей оценки совместимости и взаимосвязи стандартов и передовых методов
- практических соображений, касающиеся критериев классификации и моделей сопоставления систем.

Ниже представлены люди, сделавшие существенный вклад в работу первого рабочего

направления:

- Дженс-Тобиас Зербст, Vattenfall, Швеция
- Людовик Пйетрэ-Комбэсэдэс, Electricite de France, Франция
- Эйдж Торкилсен, SKS, Норвегия
- Оливиер Бретон, Alstom, Франция
- Симон Циммерман, Vattenfall, Германия
- Д. К. Хольстайн, OPUS Consulting Group, США
- Кристоф Пойриер, Electricite de France, Франция

4.1 Дифференцированный подход к обеспечению безопасности в электроэнергетических компаниях. Рассмотрение уровней безопасности и концепций зонирования.

Растущее число промышленных стандартов (например, [4-1], [4-2], [4-3], [4-4], [4-5]), нормативно – правовых актов ([4-6]), передовых методов ([4-7]) и проектных архитектур требует или рекомендует описания *дифференцированных подходов к обеспечению безопасности*, как надежную методологию проектирования. К сожалению, подходы к определению *дифференцированного подхода к обеспечению безопасности* в перечисленных ранее документах не упорядочены и полагаются на различные систематики, сферы деятельности и задачи.

Широкая вариативность стандартов, передовых методов и нормативно-правовых актов может привести к проблемам с согласованностью, применением и реализацией данного подхода.

Целью данной главы является уточнение понятия *дифференцированного подхода к обеспечению безопасности*, как основного принципа безопасности архитектуры цифровых систем электроэнергетических компаний. Данный принцип обеспечит эффективное снижение настоящих и будущих рисков. В данной главе будут рассмотрены следующие аспекты:

- уточнение соответствующей терминологии и определений, связанных с понятием *дифференцированного подхода к обеспечению безопасности*;
- формирование общего представления об известных стандартах и передовых архитектурах в области *дифференцированного подхода к обеспечению безопасности*;

- обсуждение их характеристик, различий и ограничений;
- демонстрация эффективности и применимости *дифференцированного подхода к обеспечению безопасности* в случае реальной атаки.

4.1.1 Термины и определения

Следующие определения разъясняют значение терминов, связанных с понятием дифференцированного подхода к безопасности.

- Дифференцированный подход к обеспечению безопасности:
  Дифференцированный подход к обеспечению безопасности – это практический подход, предназначенный для крупных распределенных вычислительных систем. В данном случае не будут применяться стандартные меры безопасности, так как их системная установка и применение экономически не эффективны. В рамках *дифференцированного подхода к обеспечению безопасности* объекты группируются по потребности в определенном виде защиты. С этой точки зрения, дифференцированный подход определяет ограниченное число *уровней безопасности*. Основываясь на группировке различных способов контроля безопасности и требованиях на различных ее уровнях, данный подход может стать основой концепции «Защиты в глубину». В рамках данной работы дифференцированная безопасность рассматривается как комплексный подход.

- Уровни безопасности:
  Уровень безопасности определяется для системы или группы систем, чтобы отразить аналогичные потребности в защите. Уровень безопасности соответствует определенному набору требований высокого уровня. Для каждой системы определяется уровень на основе списка критериев, который зависит от конкретной реализации *дифференцированного подхода к обеспечению безопасности*.

- Зона безопасности и защитное зонирование:
  Зона безопасности – это “группа логических или физических цифровых объектов, которые выделяют общие требования к безопасности. Данная зона

имеет четко определенную границу (логическую или физическую), которая отделяет включенные в систему элементы и исключенные из нее”. [4-7]

Принцип *защитного зонирования* относится к определению и применению зон безопасности (иными словами “зон”). Это часть архитектуры и реализации определенного ранее *дифференцированного подхода к обеспечению безопасности*. Каждой зоне присваивается конкретный уровень безопасности с указанием мер защиты, которые должны применяться для всех цифровых систем в этой зоне. Взаимосвязь между зонами и уровнями безопасности не является взаимно однозначной: может быть и несколько зон с одинаковым уровнем безопасности. Использование различных зон для цифровых систем, имеющих одинаковые уровни безопасности, может потребоваться для различных целей, например, для разделения административных и организационных установок, технологических сред, требующих конкретной реализации контроля безопасности, ограничения связей между зонами. В большинстве случаев при реализации контроля безопасности различные системы, входящие в одну зону, имеют надежную область связи в ее пределах, однако для управления потоком данных между зонами требуются специальные механизмы.

Зоны могут быть выстроены иерархически из набора подзон [4.7]. Разделение зон на подзоны производится по конкретным требованиям, например, по административным / юридическим потребностям, из-за технологической вариативности или для изоляции некоторых систем без ущерба для концепции перекрытия зон.

- Подход «Защита в глубину»

  Подход «Защита в глубину» часто определяется как подход к безопасности, включающий в себя многочисленные независимые меры, охватывающие организационные, технические и эксплуатационные аспекты [4-8], включаемые в принцип архитектуры безопасности, так как сами по себе они не могут обеспечить необходимый уровень безопасности. В рамках данного подхода есть множество разнообразных независимых мер, которые способны обнаружить угрозу, отреагировать и защитить систему.

В настоящее время подход «Защита в глубину» рассматривается как один из основополагающих принципов кибербезопасности, как, например, при проектировании систем [4-7], разработке программного обеспечения [4-9], в архитектурах безопасности или проектах управления безопасностью [4-10]. Согласно документу 5.71 исследовательской группы МАГАТЭ [4-11], подход «Защита в глубину» описывается следующим образом: “с точки зрения архитектуры безопасности, он включает в себя создание нескольких границ безопасности для защиты критически важных активов и сетей передачи данных от кибератак.”

Наконец, следует отметить, что понятия «Защита в глубину», *дифференцированный подход к обеспечению безопасности* и *принцип защитного зонирования* связаны между собой (иногда их даже путают). Определение подхода «Защита в глубину» перекрывает понятие дифференцированного подхода к обеспечению безопасности в том смысле, что уровни безопасности, определенные с помощью понятия дифференцированного подхода, требуют управления безопасностью, определяемого «Защитой в глубину». И именно определение различных уровней безопасности является способом диверсификации и создания нескольких уровней защиты. В рамках данной работы *дифференцированный подход к обеспечению безопасности* рассматривается как комплексный подход.

- Домены безопасности

  Объединенная рабочая группа СИГРЭ в документе D2/B3/C2 о защите информационных систем в электроэнергетических компаниях ввела *понятие домена безопасности* для электроэнергетических компаний [4-12], которое в дальнейшем было доработано рабочей группой СИГРЭ D2.22 [4-13], с использованием определения рамок доменов безопасности [4-14]. Логическая модель домена, которая требует различных уровней защиты, описана в документации рабочей группы D2.22 [4-13]. В качестве иллюстрации можно рассмотреть отображение доменов безопасности в типичной сети передачи данных в электроэнергетической компаний.

  Домен безопасности представлен в данной работе, как “среда или связь, которая определяется политикой безопасности, моделью безопасности или

архитектурой безопасности и включает набор системных ресурсов и объектов, которые имеют доступ к этим ресурсам", как описывается в ИСО 7498-2 [4-14]. Система защиты «IEC Smart Grid Standardization Roadmap» ссылается на следующие домены данной концептуальной модели: рынки, операции, поставщиков услуг, создание объема, передачи, распределение, клиентов. Данные прикладные домены являются примерами функциональных областей, которые могут быть преобразованы в *модели доменов безопасности* (метод нисходящего проектирования) [4-13] или в зонные архитектуры безопасности (метод восходящего проектирования) [4-7]. В рамках данной работы области ответственности и приемлемые уровни рисков разделяются ответственными лицами на домены безопасности. Требования безопасности выполняются благодаря дифференцированному подходу, принципам защитного зонирования и осуществлению контроля безопасности в сетях передачи данных.

4.1.2. Стандарты и передовые методы дифференцированных подходов к безопасности (от начала 2012 года)

Модель, устанавливающая значение структуры предприятия (PERA) и стандарты производственных моделей ISA95, 99	Модель, устанавливающая значение структуры предприятия (PERA) определяет Управление и Информационную Структуру, как один из трех основных компонентов предприятия, (так же выделяются Производственные Мощности, Рабочая Сила / Организация) [4-16]. Частью модели PERA является Управление и Диаграммы Информационной Структуры (CIAD), которые описывают шесть уровней проектирования и Эталонную модель для компьютерно-интегрированного производства (CIM), включающего в себя "структуру функционального иерархического компьютерного управления, спроектированную для промышленных предприятий", которая также основана на 6 уровнях. Модель PERA не поясняет понятие "дифференцированного подхода к безопасности". Однако она является основой различных стандартов и передовых методов данной области, поэтому и упомянута в данном контексте. Модель PERA была доработана и стандартизирована в документе ISA-95 [4-17]. Вышеупомянутый стандарт дает характеристику 5 уровням, определяющим границы уровней предприятия, производства и управления уровнями.

	Стандарт ISA-99, о котором будет говориться далее, так же подразумевает 5 уровней функциональной модели, полученный непосредственно из моделей PERA и документа ISA-95 при помощи изменения и реорганизации названий уровней. Данное изменение было произведено для большего соответствия анализа структуры по вопросам безопасности.
Документ по безопасности промышленной автоматизации и систем управления ANSI/ISA-99.01.01-2007 (так же известен под названием IEC 62443-11)	Серии стандартов ISA-99 “обеспечивает текущую оценку средств безопасности и технологий, которые применяются в производственной среде и системах управления” [4-7]. Стандартные серии подразумевают структуризацию документа ISA-95 с точки зрения функциональных уровней, а также вводят в первой части новые концепции безопасности, включающие уровни безопасности и зоны безопасности (как сказано в разделах 3.2, 3.3). В разработках [4-7], нет строгой фиксации числа уровней безопасности для определения несвязанных с ними критериев назначения. Но данный стандарт приводит примеры, основанные на трех несложных уровнях защиты. Более подробная концепция под названием SAL (уровни обеспечения безопасности), в настоящее время обсуждается в рамках документации ISA99 для того, чтобы перейти от качественных уровней к количественным описаниям и показателям. [4-18]
Документация 02.24, выпущенная рабочей группой СИГРЭ (Техническая брошюра 452)	В документе D2.24, разработанном рабочей группой CIGRE, образовано общепризнанное видение следующего поколения систем, связанных с энергетикой, и нацеленных в первую очередь на энергетические системы управления (EMS) и архитектуры систем управления рынка (MMS), заключенные в технической брошюре 452 [4-19]. В спецификации изложены требования к следующему поколению архитектур, которые должны предлагать ряд руководящих принципов архитектуры, соответствующих этим требованиям, в том числе рекомендациям по безопасности **(**Раздел 9). Архитектура безопасности определяет стандарты и службы

	безопасности, относящиеся к нескольким ключевым областям, которые включают в себя защиту объекта по периметру с использованием точки реализации политики (PEP) на границах области домена. Согласно документу D2.24 рабочей группы СИГРЭ [4-19], новые системы должны находиться в сетях с четко определенными зонами безопасности периметра. Их можно сгруппировать по уровням безопасности и цветной кодировке структуры безопасности.
Документация D2.22, выпущенная рабочей группой СИГРЭ (Техническая брошюра 419)	В документе D2.22, выпущенном рабочей группой СИГРЭ, разработана модель предметной области безопасности с общим уровнем защиты в отношении производимых в ней операций (см. раздел 3.5). В реальном случае уровни защиты должны быть определены, как результаты процесса управления рисками. Данные примеры приведены с целью предоставления практического руководства по развитию технологий кибербезопасности сетей передачи данных на электроэнергетических предприятиях. В таблице указаны модели, которые могут быть использованы электроэнергетическими предприятиями, а также доменами приложения, такими, как производство, передача, распределение, продажи. Домены безопасности должны быть отражены в физической сети данных электроэнергетических предприятий. Поскольку каждый домен безопасности подразумевает конкретные меры контроля, для размещения системы могут быть выбраны определенные технологии безопасности. Приведены примеры технологий обеспечения безопасности для корпоративного домена, а также примеры дополнительных технологий, которые необходимы для обеспечения безопасности критически важных для бизнеса и функционирования доменов.
	Национальный институт стандартов и технологий (НИСТ) в специальной публикации 800-82 “Руководство по защите систем управления промышленными процессами” описывает методы защиты и управления безопасностью. В частности, в данном документе поясняется такой вид защиты

Документ НИСТ (специальная публикация 800-82)	архитектуры, как подход “Защита в глубину” [4-20], где приведены ссылки на документ национальной лаборатории штата Айдахо, который называется “Защита управления кибер-системами: стратегии защиты в глубину” [4-21]. Документ “показывает традиционное разделение корпоративных архитектур и доменов управления” и представляет зонную модель. Кроме того, здесь описаны и визуализированы дополнительные типы атак. В заключении приведены различные меры безопасности. В октябре 2009 года, документ был обновлен [4-22], в результате чего была добавлена пятая зона для защиты инструментальных систем.
Руководство по регулированию 5.71 Комиссии по ядерной регламентации США (NRC)	Руководство 5.71 [4-5] описывает регулирующую статью, пропагандирующую стратегию защиты, которая включает архитектуру безопасности и набор элементов управления безопасностью на основе стандартов, предусмотренных в специальных публикациях 800-53 и 800-82 комиссии НИСТ, “Руководство по защите промышленных систем управления” [4-20]. Одна часть руководства 5.71 дает определение защитным уровням и концептуально соответствует существующим областям физической безопасности, а также описывает пример архитектуры безопасности: “Данная архитектура безопасности включает в себя пять концентрических уровней надзора за кибербезопасностью, разделенных границами безопасности. Например, межсетевая защита, диоды, благодаря которым цифровые сигналы связи могут находиться под контролем и ограничением” [4-5]. “Примером такого вида архитектуры безопасности являются те системы, которые включают в себя ряд концентрических защитных уровней повышения безопасности. Эти уровни концептуально соответствуют существующим областям физической безопасности объекта” [4-5 - C.3.2.1]
	Институт ядерной энергии – это американская организация, определяющая политику в области энергетики и индустрии высоких технологий в США. Институт и его сотрудники разрабатывают политику в отношении ключевых законодательных и нормативных

Политика Института ядерной энергии США (NEI) 08-09	вопросов, влияющих на данную отрасль. Так же, Институт ядерной энергии принимает активное участие в сфере кибербезопасности: в 2005 году он выпустил руководство NEI 04-04 по кибербезопасности атомных электростанций США. После выпуска нового постановления в 2009 году (глава 10 Свода Федеральных постановлений США (CFR), параграф 73.54), руководство NEI 04-04 было заменено на NEI 08-09 от 2010 года (шестая версия документа), которое будет применяться на предприятиях США, использующих ядерную энергию, в качестве базы для разработки плана кибербезопасности критически важных цифровых ресурсов. Данный формат ориентирован на соблюдение правил, установленных Комиссией по ядерной регламентации США в области кибербезопасности.
Справочное руководство по компьютерной безопасности на ядерных объектах (Международное агентство по атомной энергетике)	Международное агентство по атомной энергетике (IAEA) подготовило новый проект, касающийся компьютерной безопасности на ядерных объектах. После нескольких лет дискуссий, он находится на последней стадии разработки перед публикацией на момент написания этой статьи. Целевая аудитория данного проекта достаточно обдирная и включает регулирующие органы, политиков, операторов систем и поставщиков. Область применения также велика, поскольку документ содержит рекомендации по организационным вопросам и вопросам реализации, что касается безопасности всех типов цифровых систем, которые находятся в области атомной энергетики, в том числе IT-системы и промышленные системы управления. В частности, здесь рекомендуется использование дифференцированного подхода и принципов зонирования на подобии описания, приведенного в разделах 3.1 и 3.3. Примером реализации может послужить определение пяти уровней безопасности с растущими требованиями, а также набор общих требований, которые должны применяться ко всем системам.
	При содействии подкомитета 45A, Международный электротехнический комитет (МЭК) утвердил стандарты для

Проект МЭК 62645	оборудования атомных станций и систем управления. Им выпущены широко используемые и общепризнанные серии систем безопасности. МЭК 61226 - самый популярный стандарт среди них. В нем описана классификация безопасности. Совсем недавно, МЭК подкомитета 45А использовался как международный стандарт по кибербезопасности измерительных приборов и систем управления АЭС. В настоящее время, находясь на стадии разработки, он также призывает к использованию дифференцированного подхода к обеспечению безопасности, определений уровней безопасности и связанных с ними требований. В данном проекте определены три уровня безопасности (называемые степенями). Они определяются на основе выводов об общем состоянии безопасности станции и эффективности каждой рассматриваемой системы. Здесь используются существующие классификации безопасности, определенные в МЭК 61226. Данная классификация является основой при присвоении степени безопасности; тем не менее, не существует однозначного соответствия между степенью безопасности и классами безопасности. Все остальные аспекты безопасности здесь не будут иметь значения. Кроме того, нет прямого соответствия между степенью безопасности и уровнями, изложенными в документе ISA-95 модели PERA. Обратите внимание, что определение степени безопасности может изменяться в процессе стандартизации. Мы не будем рассматривать это в рамках данной статьи.
Проект «SeSa» Фонда научных и промышленных исследований	Группа фонда научных и промышленных исследований (The SINTEF Group) является прикладной научно-исследовательской организацией в Скандинавии. В рамках проекта «SeSa» (обеспечение безопасности) были разработаны системный и методологический подходы к ответу на вопрос является ли приемлемым данное решение для удаленного доступа к Объединенной европейской информационной системе (SIS). [4-23] Данная информация резюмируется в отчете организации SINTEF [4-23]. Основой организации SINTEF являются оффшорные операции, например, добыча нефти на шельфе. В отчете описана

	“многоуровневая модель для удаленного доступа”, которая включает 7 уровней.
Требования системы безопасности развитой инфраструктуры измерений (AMI)	Целью описания безопасности развитой инфраструктуры измерений (AMI) является обеспечение коммунального хозяйства, сообщества поставщиков и других заинтересованных лиц набором требований к безопасности, которые должны быть применены при создании развитой инфраструктуры измерения. Это обеспечит высокий уровень безопасности, необходимый для поддержания надежной защиты и доверие потребителей” [4-24]. Данный документ содержит описание модели домена безопасности как “созданной для ограничения сложности обеспечения безопасности, что необходимо для создания надежной и безопасной инфраструктуры измерения. Кроме того, он может использоваться как инструмент для управления системами обеспечения. Требования к безопасности указаны в документации по применению развитой инфраструктуры измерений” [4-24]. 17 декабря 2008 года версия 1.01 рассматривалась в качестве требований к системам безопасности развитой инфраструктуры измерений.

Таблица 4-1: Стандарты и передовые методы дифференцированного подхода к безопасности (на начало 2012 года)

Название документа	Тип/Цель	Документ	Число уровней безопа-сности	Управ-ление безопасностью	Терми-нология	Ссыла-ется на/ основан на	После-дняя версия
PERA Модель ISA95	Бизнес-архитектуры /Интеграция	Модель	6	Отсутст-вует	Уровни	-	1989 (PERA) 2000 (ISA95)
Стандарт ISA99	Безопа-сность	Внут-ренний	3+	Синхро-низация,	Уровни, зоны,	Анализ рисков	2007

	интегрированной системы управления и контроля	стандарт		деление (сегментация)	подзоны, синхронизация		
Документ СИГРЭ D2.22	Методические рекомендации по безопасности электроэнергетических предприятий	Техническая брошюра	4	Есть (высокий уровень)	Домены безопасности, уровни защиты	СИГРЭ Объединенная рабочая группа D2/B3/C2	2011
Документ СИГРЭ D2.24	Безопасность интегрированной системы управления и контроля	Техническая брошюра 452	5	Есть	Зоны защиты, уровни безопасности	Регион INL	2011
Комиссия по ядерной регламентации США (NRC) Руководство 5.71	Безопасность интегрированной системы управления и контроля ядерных установок	Руководство	5	Есть	Уровни	-	2010
МЭК 61645	Безопасность интегрированной системы управле-ния и контроля для ядерных установок	Первый международный стандарт (проект)	3	-	-	-	Проект

НИСТ Специальная публикация SP800-82	Безопасность интегрированной системы управления и контроля	Руководство США (доступен окончательный проект)	-	Есть	Зоны, «Защита в глубину»	PERA	Публикация итогового проекта (2008)
Фонд научных и промышленных исследований (проект SeSa)	Архитектура безопасности интегрированной системы управления и контроля	Проектная документация	7	Есть	Зоны	МЭК 61508, Общие критерии	2007
Документ NEI 08-09 Института ядерной энергии	Безопасность интегрированной системы управле-ния и контроля для ядерных установок	Руководство США (принято для соблюдения регулирования)	4	Есть (детальное)	Уровни безопасности	-	Проект
Справочное руководство Международного агентства по атомной энергетике (IAEA)	Безопасность интегрированной системы управления и контроля для ядерных установок	Руководство (проект)	5	Есть (высокий уровень)	Уровни безопасности	-	Проект
Требования системы безопасности и развитой инфраструктуры измерений (AMI)	Безопасность интегрированной системы управления и контроля	Документ	5	Есть	Домен безопасности	-	2008

Таблица 4-2: Сравнение стандартов и передовых методов (на начало 2012 года)

4.1.3. Пример дифференцированного подхода к безопасности для подавления усовершенствованных кибератак.

Чтобы отразить эффективность *дифференцированного подхода к обеспечению безопасности*, в данном разделе мы оценим воздействие теоретически возможной серьезной многовекторной атаки на упрощенную архитектуру. Данная архитектура реализует дифференцированный подход к обеспечению безопасности и принцип защитного зонирования так, как это описано в разделах 3.1 и 3.3. Выбранные направления атаки соответствуют работе вредоносного программного обеспечения «Stuxnet» [4-25].

Исходя из поставленных целей, в данном разделе рассматриваются:

- Краткое описание атак вируса «Stuxnet»;
- Идентификация возможных точек атаки данных векторов в упрощенной архитектуре, разработанной исходя из дифференцированного подхода к безопасности;
- Примеры защитных мер; объяснение ожидаемого поведения архитектуры при рассматриваемых видах атак.

Данные элементы рассматриваются лишь для того чтобы пояснить применение и эффективность дифференцированного подхода к обеспечению безопасности, основываясь на конкретных примерах. Они не представляют собой детально описанные случаи или руководство, не являются универсальными, полными или исчерпывающими.

4.1.3.1 Процессы атаки

Ссылаясь на текущую общедоступную информацию, вирус «Stuxnet» основывается на следующих программных методах:

i. Распространение через сетевые программы: заражение систем WinCC через код доступа к серверу базы данных;
ii. Распространение через сетевые программы: распространение через сетевые ресурсы;
iii. Распространение через сетевые программы: распространение через уязвимые места службы MS08-067 Windows-сервера;
iv. Распространение программ: передача данных между узлами, обновление данных[4];

[4] Нет прямого распространения программы

v. Распространение программ: распространение с использованием уязвимости в службе диспетчера очереди печати MS10-061;
vi. Распространение через съемный диск: уязвимость системы LNK (CVE-2010-2568) или AutoRun.Inf;
vii. Седьмой шаг проекта о заражении фалов: файлы S7, MCP или TMP.

4.1.4. Сравнение инфраструктуры интегрированной системы управления и контроля с помощью рассмотренных процессов атаки.

На рисунке 5-2 приведен высокоуровневый и упрощенный сценарий того, как атаки могут повлиять на инфраструктуру интегрированной системы управления и контроля, разделенную на зоны безопасности. Данный сценарий не отображает полную или детальную визуализацию, а лишь эффективность дифференцированного подхода к обеспечению безопасности. Красные числа обозначают методы, перечисленные в предыдущем разделе. Сценарий нагляден, так как на рисунке показаны только основные варианты атак.

4.1.5. Варианты мер защиты в дифференцированном подходе к безопасности

Для того, чтобы оценить влияние дифференциального подхода к обеспечению безопасности, необходимо применять к различным зонам следующие контроллеры безопасности.

i. Физическое разделение систем, например, воздушный зазор, физическое ограничение для организации передачи информации только в одну сторону (Зона E)
ii. Логическое разделение функционально связанных систем в связи с требованиями приложений, например, межсетевой экран, глубокая проверка передаваемых пакетов (Зона D)
iii. Ограничение доступа в сеть Интернет (Зоны B, C, D)
iv. Система / Зона укрепления защиты с помощью уровней требований (Зоны A, B, C, D, E)
v. Управление специальными системными / зонными патчами для системных типов / уровней требований (Зоны A, B, C, D, E)
vi. Ограничения, накладываемые на переносные носители, например, организационные или технические ограничения на USB- или CD-носители (зона D)

vii. Ограничение на подключение с рабочей станции к сегментам сети (Зоны B, D)

viii. Ограничение на дистанционное обслуживание сторонней организации (Зона D)

ix. Применение антивирусного сканера (Зоны A, B)

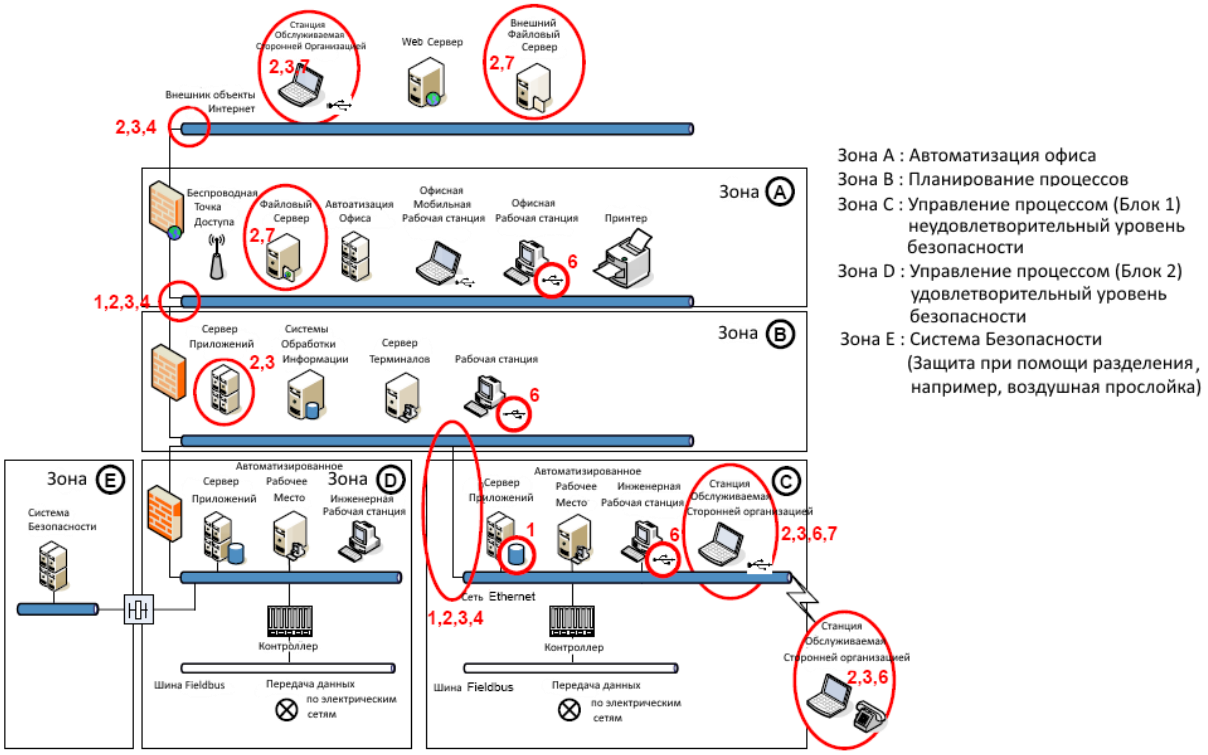

Рисунок 4-1 Упрощенный пример архитектуры предприятия, демонстрирующий различные виды атаки

4.1.6. Оценка эффективности дифференцированного подхода к обеспечению безопасности

На основе рассмотренного воздействия модели атак на упрощенную архитектуру можно сделать следующие выводы о дифференцированном подходе к обеспечению безопасности:

- Изоляция или сетевое разделение выступает как подавление влияния вирусов между безопасными зонами. В качестве примера, обратите внимание на Зоны D и E. Важное значение имеет эффективность реализуемых мер безопасности, определяющих дифференцированный подход к обеспечению безопасности, например, разделение зон при помощи брандмауэра или правил передачи данных.
- Применение множества средств контроля безопасности в различных зонах дает возможность создать адаптированную и достаточно безопасную практическую реализацию. Например, ограничение на использование USB портов только в

зонах D и E. Данное ограничение отсутствует в зонах A и B, так как наличие антивирусного сканера можно считать достаточным для предотвращения USB-атак.

- Дифференцированный подход к обеспечению безопасности позволяет использовать лучшие методы контроля: например, рассмотрим антивирусный сканер в зонах A и B. Можно заметить, что он отсутствует в зонах D и C ввиду некоторых системных характеристик или неполной реализации системы.
- Нарушения при использовании дифференцированного подхода к обеспечению безопасности могут привести к падению всей системы безопасности. Например, поддержка рабочей станции сторонней организацией в зоне C.

4.1.7. Заключение

Электроэнергетические предприятия сталкиваются с новыми проблемами с точки зрения кибербезопасности, вызванные быстрым развитием данной области и технической инфраструктуры. Многочисленные стандарты, передовые методы, проектные архитектуры явились толчком для создания дифференцированного подхода к обеспечению безопасности, внедрения зон безопасности. Основываясь на определении различных стандартов, передовых методов и проектных архитектур, связанных с дифференцированным подходом к обеспечению безопасности, можно сделать следующие выводы:

- В рассматриваемых документах терминология и определения, связанные с дифференцированным подходом к обеспечению безопасности, имеют некоторые отличительные особенности. На практике это может привести к трудностям при сопоставлении, применении и реализации. Тем не менее, большинство рассматриваемых документов содержат сложные понятия и принципы, приведенные в данной статье;
- Развитие дифференцированного подхода к обеспечению безопасности не должно изучаться изолированно от других аспектов работы предприятий. Практическая реализация и эксплуатация данного подхода к безопасности также должна включать аспекты, не относящиеся к безопасности, например, целостность корпоративных данных, архитектуру, управление, организационные структуры, физическую среду, правовое регулирование, правила техники безопасности. Все эти аспекты должны быть учтены и приведены в соответствие с

дифференцированным подходом к обеспечению безопасности для успешного и эффективного внедрения и эксплуатации;

- Необходимо обеспечить критерии классификации, чтобы осуществить последовательное отображение цифровых систем в различных зонах, и предоставить, таким образом, успешную реализацию дифференцированного подхода. В изученных документах критерии классификации представлены не в полном объеме.

  Далее следовало бы сказать, что критерии классификации безопасности не должны приводить к несоответствию с характеристиками, не относящимися к безопасности, которые были упомянуты ранее;
- Эффективность дифференцированного подхода к обеспечению безопасности основывается на соответствующем выборе, реализации и эксплуатации различных мер безопасности. Поэтому контроль безопасности не может быть сведен лишь к мерам сетевого разделения, но при этом необходимо применить средства управления безопасностью различного уровня такие, как организационные, физические, технические, уровень защиты в глубину.

4.2 Методология классификации дифференцированных подходов к обеспечению безопасности в архитектурах электроэнергетических компаний

Применение «дифференцированного подхода к обеспечению безопасности» сегодня признается как широко используемый принцип обеспечения безопасности структуры для защиты цифровых систем и потенциально опасных объектов жизнеобеспечения информационных технологий в электроэнергетических компаниях. Различные промышленные стандарты, правила, и передовые практики применяют метод «дифференцированного подхода к обеспечению безопасности», вводя «принципы зонирования» или «структуру защиты домена» и объединяя требования соблюдения безопасности на разных уровнях защиты. (См. стандарт МЭК 62443 [4-26], техническое руководство МАГАТЭ «Компьютеры на ядерных объектах» [4-27], руководство Комиссии по ядерному регулированию 5.71 [4-28], Североамериканская корпорация электрической надежности: исследование надежности вследствие объединения умных сетей электроснабжения [4-29], и т. д.)

К сожалению, объединенной методологии классификации, критериев классификации или процедур, нацеленных на успешное внедрение и сохранение «дифференцированного

подхода к обеспечению безопасности» недостает, в то время как методологии, описанные в существующих документах несодержательны и, в основном, незакончены. Недавний труд от рабочей группы D2.31 из СИГРЭ перечислил и проанализировал большое количество этих рекомендаций и отметил немало несоответствий и незавершенность. [4-30].

В данном параграфе речь пойдет о практической методологии внедрения «дифференцированных подходов к обеспечению безопасности». В дальнейшем в работе объединены соответствующие критерии классификации и приведены выводы с примерами.

4.2.1 Методология внедрения «дифференцированного подхода к обеспечению безопасности»

При использовании «дифференцированного подхода к обеспечению безопасности» в структуре информационных технологий электроэнергетических компаний, должны быть созданы технические, организационные и физические органы управления, поддерживаемые в рабочем состоянии.

Схема жизненного цикла может применяться для структурирования процесса внедрения дифференцированного подхода к обеспечению безопасности и для обеспечения тесной интеграции со всеохватывающей методологией жизненного цикла в реализации и работе цифровой системы. Следующий план дает представление о различных стадиях реализации «дифференцированных подходов к обеспечению безопасности» применительно к схемам жизненного цикла как, например, МЭК 61508 безопасный жизненный цикл [4-31] или «управление жизненным циклом безопасности», описанным в техническом руководстве МАГАТЭ «Компьютеры на ядерных объектах» [4-27, с. 15].

a) Понятие модели зоны в качестве основы для реализации цифровой системы: модель зоны является архитектурной реализацией «дифференцированного подхода к обеспечению безопасности» в техническом, организационном и физическом смысле. Под зоной может пониматься набор логических или физических активов, к которым предъявляются общие требования (ср. [4-29], [4-26]). Зона включает в себя набор определенных элементов управления, которые применяются для всех цифровых систем, расположенных внутри зоны. В существующих инфраструктурах (например, заводской

инфраструктуре, инфраструктуре электроэнергетических компаний, реализации цифровых систем / поставки) архитектурная концепция, в целом, существует. Эта концепция может также включать в себя модель зоны, основанную на главных характеристиках и ограничениях, как, например,

- Тип производства / операции (например, распределение, передача, производство тепловой энергии, ядерная энергетика и т.д.)
- корпоративная политика и характеристики
- национальные или международные требования (например, Североамериканская корпорация электрической надежности (NERC): критическая защита инфраструктуры (CIP) [4-32])
- стандарты или передовые практики (например, МЭК 62443-1 [4-26], Комиссия по ядерному регулированию 5,71 [4-28], межведомственный отчет Национального института стандартов и технологий (NISTIR) 7628: руководство по кибербезопасности «Умных сетей» [4-33], Grundschutz-стандарт информационных технологий [4-34])
- планы поставки (например, [4-35], [4-36])

Существующая реализация модели зоны является основой для описанного поэтапно подхода (b) - (f). Если она достаточна, то следует установить основы для реализации цифровой системы. Если достаточная модель зоны не существует в инфраструктуре или новая инфраструктура должна быть создана (например, новый строительный проект), модель зоны должна быть определена на этапе (d), посредством группировки логических или физических активов, которые имеют общие требования и определения необходимых элементов управления зоны, (ср. [4-26])

b) Определение цифровых систем или набора функций, которые являются объектом для анализа.

c) Анализ и оценка цифровых системных и функциональных компонентов: Функциональные и цифровые компоненты системы анализируются и оцениваются для определения требований и определения возможного уровня безопасности (также иногда называют «Спецификация системных требований»). Критерии классификации поддерживают стандартный способ определения требований и обеспечивают тем самым охват соответствующих частей, таких как определение и оценка потенциальных опасностей и рисков.

Кластерные критерии классификации служат, например, для оценки риска, анализа воздействия, оценки технико-экономических обоснований, архитектуры и т.д..

d) Назначение цифровой системы в выделенной зоне или подзоне[5] в заранее определенной модели зоны: на основании *результатов анализа и оценки цифровых системных и функциональных компонентов* цифровые системы классифицируются в выделенную зону для того чтобы обеспечить общее выполнение требований по техническим, организационным и физическим органам управления, подразумевающих специфический набор управления и архитектуру зоны. Отображение в зону может быть описано как часть системного дизайна высокого уровня и, следовательно, является частью этапа реализации развития системы.

e) Выделенные органы управления цифровой системой: несоответствия между установленными требованиями к цифровой системе и прикладными органами управления зоны должны быть определены для обеспечения надлежащего смягчения последствий со стороны специализированных систем управления. Если смягчение не представляется возможным (например, допустимый риск превышает предел) среди прочих могут быть применены следующие методы:
   - Повторная оценка систем или окружающих систем,
   - Адаптация конкретного набора органов управления зоны,
   - переоценка проекта системы, действующей модели,
   - переоценка модели зоны более высокого уровня.

   Анализ расхождений и определение выделенных элементов управления системы могут быть описаны как часть *детального проектирования системы.*

f) Другие этапы жизненного цикла, такие как части этапа реализации (например, запуск тестирования допустимости) или рабочий этап не обсуждаются далее в этом пункте.

На основе поэтапного осуществления «дифференцированного подхода к обеспечению безопасности» в этом документе излагаются ключевые моменты для поддержки его практической реализации:

- определение соответствующих критериев классификации
- практическая методология определения системы для выделенных зон
- применение методологии на примерах

[5] Зона или «подзона» далее по тексту только как «зона»

4.2.2 Определение соответствующих критериев классификации

Сутью «дифференцированного подхода к обеспечению безопасности» является установление различных зон, и определение цифровых систем или функций[6] для этих зон. Критерии классификации характеризуют требования цифровых систем и, следовательно, оказывают существенное влияние на применяемые элементы управления, в основном, на использованные архитектуру, эксплуатацию, обслуживание и т.д. ..

4.2.3 Обсуждение существующих стандартов и передовой практики

Чтобы сделать возможным сравнение и дальнейшее обсуждение критериев классификации согласно действующим стандартам и передовым практикам, рабочая группа СИГРЭ D2.31попыталась сгруппировать критерии классификации. Приведенные кластеры получены из трехслойного представления[7] [4-37] языка ArchiMate.

- Бизнес-слой сообщает о бизнес-процессах, услугах, функциях и событиях, происходящих в филиалах фирм. В контексте «дифференцированного подхода к обеспечению безопасности» бизнес-слой приведен к таким критериям, как безопасность, эксплуатационная уместность, влияние на производственные и бизнес-процессы.
- Уровень приложений содержит информацию о программных приложениях, которые поддерживают компоненты совместно со службами приложений. В контексте «дифференцированного подхода к обеспечению безопасности» уровень приложений адаптирован к таким критериям, как категории приложений, например, сервер сбора данных, сервер приложений, истории, базы данных, ЧМИ и т.д.
- Технологический уровень связан с аппаратной и коммуникационной инфраструктурой для поддержки уровня приложений. В контексте «дифференцированного подхода к обеспечению безопасности» технологический уровень адаптирован к таким критериям, как сетевые категории, например, система управления LAN.

На основе этих кластеров рабочая группа СИГРЭ D2.31 проанализировала выбранные

---

[6] «цифровые системы или функции» далее по тексту только как «цифровые системы»

[7] ArchiMate, стандарт Open Group, является методологией построения предприятия и основой для повышения эффективности бизнеса.

стандарты и передовые практики для критериев классификации, критериев зоны и/или управления, чтобы организовать «дифференцированный подход к обеспечению безопасности». На рисунке 1 представлена сводка этого анализа, показывающая приоритетную зону различных стандартов и передовой практики.

В результате делается вывод, что стандарты и передовые практики охватывают и сосредотачиваются на разных целевых группах, областях применения и характеристиках «дифференцированного подхода к обеспечению безопасности». Далее можно заключить, что всеобъемлющей нормализации критериев классификации не существует. Вышесказанное может также применяться к общему определению набора управления, примененному в «дифференцированном подходе обеспечения безопасности» или обычной модели зон.

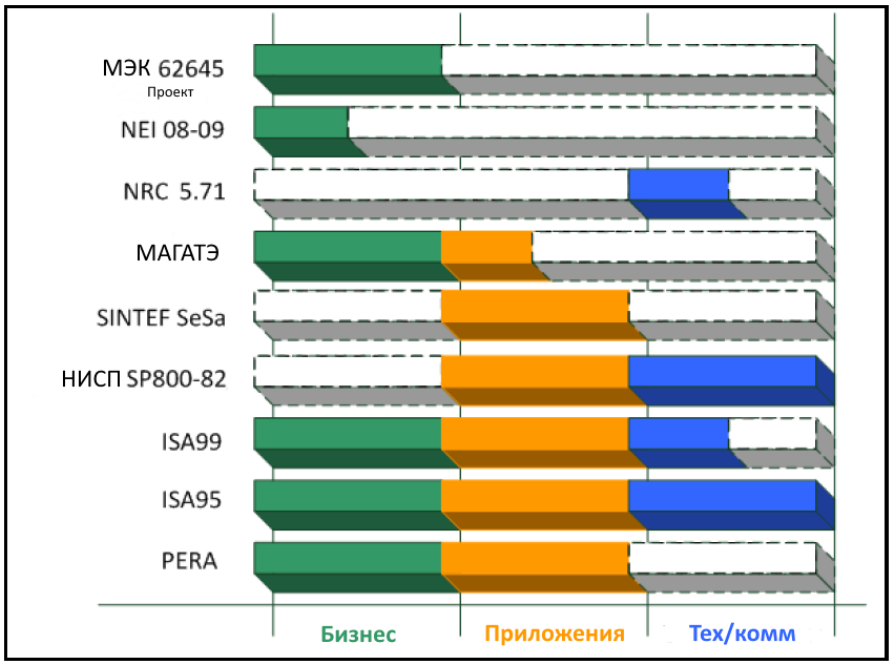

Рисунок 4-2 Приоритетная область критериев кластера в соответствии со стандартом

Однако для конкретной архитектуры, рабочего процесса или производственной сферы, такой как «Умная сеть» общее определение «дифференцированного подхода к обеспечению безопасности» и набор соответствующих требований представлялись бы возможными, и можно было бы установить общие уровни безопасности, интерфейсы или правила соответствия (см «Немецкий защитный профиль для модуля безопасности входа смартметра» [4-38], ср. [4-39]), сравнимые с другими отраслями (см [4-40]).

4.2.4 Практическая методология классификации систем на соответствующие зоны

Критерии классификации должны учитывать все функциональные, технические, эксплуатационные требования и требования безопасности цифровой системы, функции или архитектуры. Сведение критериев классификации к одному лишь обсуждению безопасности, не принимая во внимание окружающие элементы, может привести к ограничениям и противоречиям в требованиях и принципах проектирования. Например, требования безопасности могут вступать в конфликт или усиливать друг друга в зависимости от ситуации [4-41]. Опыт показал, что такие ситуации вызывают осложнения, задержки, ненужные затраты или обходные пути на стадии реализации, эксплуатации и технического обслуживания цифровых систем при внедрении «дифференцированного подхода к обеспечению безопасности».

> *Пример: Распределенная сеть представляет собой совокупность островов автоматизации, без возможности взаимодействия за пределами их границ, а «Умная сеть» позволит системам взаимодействовать между собой. С одной стороны, эта интеграция необходима, например, для улучшения соотношения источников энергоснабжения с потребителями и повышения возможности самовосстановления, но, с другой стороны, опираясь на инфраструктуру связи и информационные технологии, энергосистема становится более уязвимой для кибератаки. Поэтому должен существовать точный баланс между рабочими требованиями и требованиями безопасности.*

Применение критериев классификации, охватывающих все соответствующие области для внедрения, эксплуатации и обслуживания «дифференцированного подхода к обеспечению безопасности» должно снизить этот риск. На рисунке 2 показаны целостные критерии классификации кластеров, основанные на трех принципах: технологии, бизнеса и приложений, полученных из языка моделирования ArchiMate [4-37].

Первое наложение этих принципов относится к поведению системы, информации и структуре. На основании этого наложения внешняя оболочка представляет собой восемь категорий, охватывающих возникающие области «дифференцированного подхода к обеспечению безопасности»:

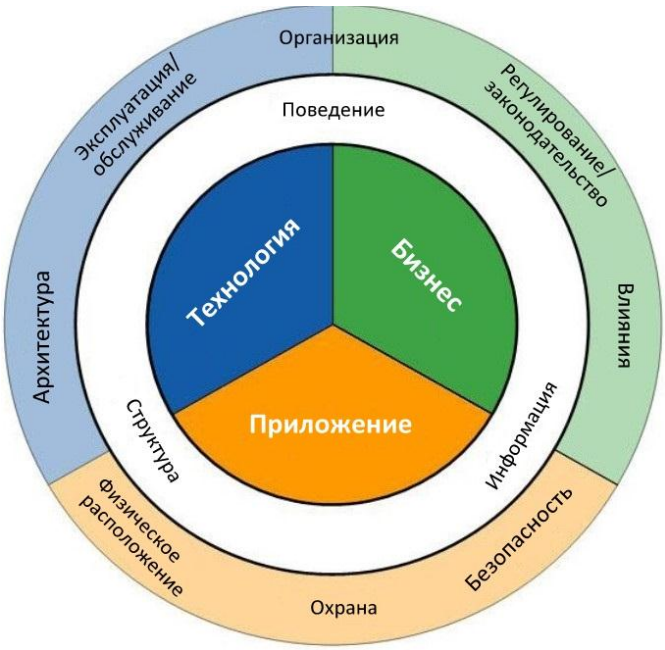

Рисунок 4-3 Категории критериев классификации

- Правила / Законодательство: Цифровая система должна соответствовать различным правилам и законам в соответствии с местными, региональными, национальными или международными законами и стандартами.
- Воздействие: анализ воздействия на бизнес и оценка риска определяют последствия возможной неисправности цифровой системы (например, недоступность, ненадежность, потеря данных, неправильное использование и т.д.), влияющей на бизнес или производственный процесс. Итоги анализа воздействий и оценка риска отражены в требованиях.
- Безопасность: Цифровая система может поддерживать функцию безопасности, работу и процессы. Стандарты безопасности (например, МЭК 61508 [4-31]) определяют запросы к этим цифровым системам, которые отражены в требованиях.
- Информационная безопасность: определены требования безопасности (например, в соответствии с конфиденциальностью, целостностью и доступностью анализа воздействия), основанные на оценке риска.
- Физическое расположение: Физическое расположение цифровой системы необходимо учитывать и устанавливать требования не только к модели зоны более высокого порядка, но и к цифровой системе.
- Архитектура: Цифровая система базируется на архитектуре технической системы. Тем не менее, она также является частью ландшафтной архитектуры и, в то же время, объединена с ней, что технически реализуемо, но ставит ограничение на

цифровую систему. И общие, и специальные технические требования необходимо оценивать.

- Рабочий процесс / Техническое обслуживание: Модель рабочего процесса и технического обслуживания цифровой системы, технический ландшафт или окружающая инфраструктура могут установить требования не только к модели зоны более высокого порядка, но и к цифровой системе.
- Организация: Цифровая система интегрирована не только в информационную технологию, бизнес или производственный ландшафт, но и в организационную структуру, которая помогает ей, но и ограничивает.

4.2.5 Применение метода «Пути перемещения» для определения возможной целевой зоны

Одним из факторов успеха при реализации всеобъемлющего «дифференцированного подхода к обеспечению безопасности», интегрируемого в организацию или завод, является создание единой методологии классификации, которая обеспечивает согласованность, даст практические рекомендации, и учтет соответствующие требования цифровой системы и окружающей архитектуры. Изложенная методика представляет собой практический способ реализации дифференцированного подхода к обеспечению безопасности в среде электроэнергетических компаний.

В основе описанной методологии лежит список вопросов, охватывающих соответствующие области категорий критериев классификации. Список может включать в себя многочисленные вопросы в каждой категории классификации для обеспечения достаточного пояснения.

Пример: Для освещения 4-х «Р» модели PERA Enterprise [4-42] список включает такие вопросы, чтобы определить требуемое «время отклика» (*response time), «время разрешения» (resolution time), «надежность» (reliability) и «ремонтопригодность» (reparability) цифровой системы или функции.*

Для каждого вопроса возможная зона или диапазон зон определяются на основании данного ответа.

Пример: Если требуемые «время отклика», «время разрешения», «надежность» и «ремонтопригодность» цифровой системы составляют "дни или недели", согласно

модели PERA Enterprise целевая зона будет "5". Если требуемые «время отклика», «время разрешения», «надежность» и «ремонтопригодность» составляют "миллисекунды или секунды", в соответствии с моделью PERA целевая зона будет "1".

На основании этой информации (ответы на определенные вопросы из каталога) путь перемещения (ср. [4-43]) может окончательно определить возможную целевую зону (или диапазон нескольких целевых зон). Если результатом является диапазон нескольких зон, будет выбрана наиболее «дешевая» зона. Ранжирование зон по «стоимости» должно быть адаптировано к специальным требованиям и ограничениям. На рисунке 3 изображено применение каталога вопросов (Q1, Q2, ..., Qn), относительно предлагаемой целевой зоны (диапазона нескольких зон) на основании ответа (A1, A2 ..., An) и применение пути перемещения.

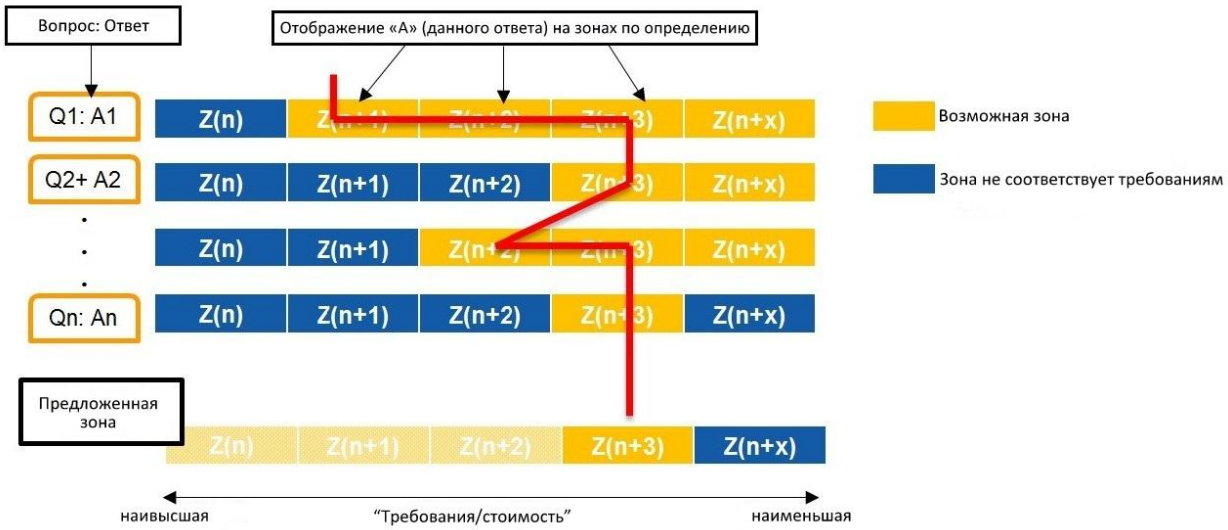

Рисунок 4-4 Применение метода «Пути перемещения» для определения целевой зоны

Иногда, основываясь на ответах из списка, ни одна из зон не может быть предложена автоматически. В этом случае проект должен быть перенастроен вручную, либо путем изменения ограничений и, следовательно, ответов в вопроснике выбора зоны, или путем выбора наиболее подходящей зоны и, применением соответствующих средств управления системой. В любом случае, как следствие из струнного определения, результат может дать только указание и должен быть проверен вручную.

4.2.6 Применение методологии на примере

Пример показывает классификацию цифровой системы относительно модели зоны с 4 + n зонами на основе выборочных неисчерпывающих вопросов в *области воздействия,*

информационной безопасности, охраны и архитектуры. Вопросы и ответы носят гипотетический характер, но должны дать представление о том, каким образом эта методология может быть применена на практике для определения предлагаемой целевой зоны.

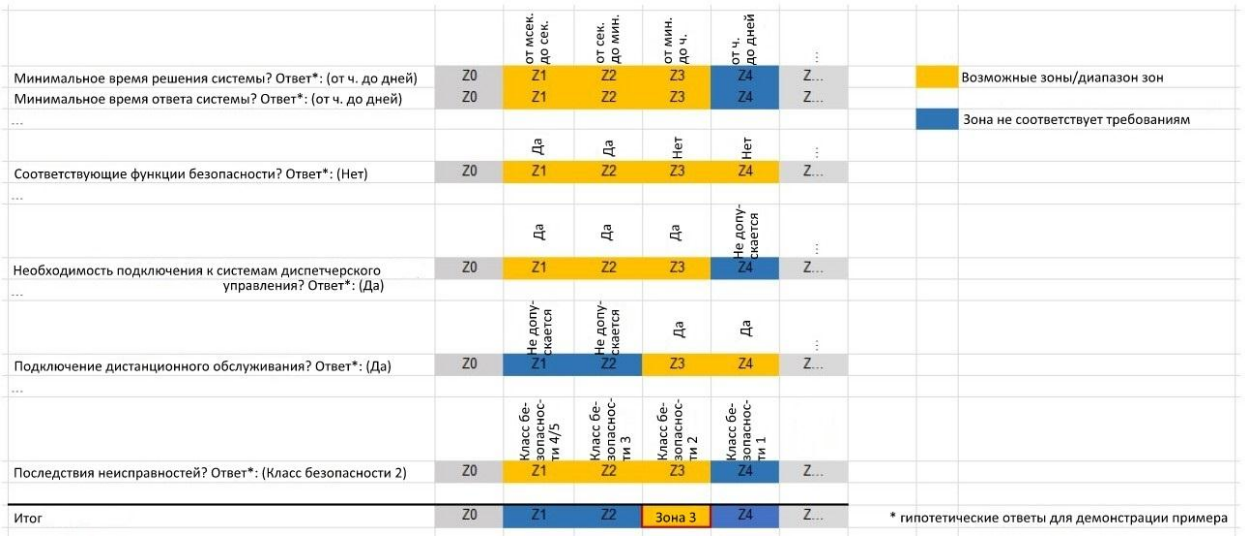

Рисунок 4-5 Применение подхода на 6 примерных вопросах

4.2.7 Заключение

Успех «дифференцированного подхода к обеспечению безопасности» зависит от эффективности реализации, обслуживания и эксплуатации. Практические методологии, руководящие принципы, шаблоны и ссылки на стандарты и передовые практики необходимы, для облегчения процесса внедрения «дифференцированного подхода к обеспечению безопасности» и в целях обеспечения соответствия. Эффективная практическая методология для ввода дифференцированного подхода к обеспечению безопасности в архитектурах электроэнергетических компаний заключается в разработке и реализации подхода к классификации, который непосредственно относится к бизнесу, технологиям и применению в электроэнергетических компаниях.

В дополнение можно отметить, что методология более быстрого проекта «дифференцированного подхода к обеспечению безопасности» может снять бремя проверки безопасности указанием на критическое распределение систем, которое требует создания некоторых специальных элементов управления. Для увеличения результативности, следующим шагом может стать создание общего определения «дифференцированного подхода к обеспечению безопасности» и набора требований для конкретных областей в умных сетях электроснабжения.

5 Второе рабочее направление: характеристика, классификация и моделирование угроз безопасности.

Целью данного рабочего направления является разработка и анализ следующих аспектов:

- Подходы к графическому моделированию атак, относящихся к вопросам ЭЭК;
- Вспомогательный анализ оказываемых последствий при внедрении доступных решений умных сетей и поддержка дополнительного внедрения соответствующих защитных мер по усилению безопасности;
- Связь между моделированием атак и полным анализом рисков инфраструктуры защиты для оптимизации построения мер защиты;

Ниже представлены люди, сделавшие вклад в разработку второго рабочего направления:

- Джованна Дондосола, Исследование энергетических систем, Италия
- Матиас Екстед, Королевский технологический институт, Швеция
- Лудовик Пйетрэ-Комбэсэдэс, Electricite de France, Франция
- Джон Макдональд, Electricite de France, Франция
- Матус Кормэн, Королевский технологический институт, Швеция
- Робэрта Терруджиа, Исследование энергетических систем, Италия
- Эйдж Торкилсенг, SKS, Норвегия

Для дальнейшего определения принципов построения архитектуры рабочее направление 2 берет основу с моделирования кибератак для оценки безопасности умных сетей.

Развитие умных сетей будет иметь возможность предоставлять многочисленные услуги с новыми моделями трафиков. Данные разработки радикально изменят как возможности доступа к сетям, так и основные архитектуры, и технологии. Скорее всего, умные сети будут являться топологически сложными, содержать большое количество неоднородных граничных точек, участников, интерфейсов, каналов связи, эксплуатационных режимов и запрашивать принципы действия, охватывающие различные области, требующие знания и профессиональный опыт ИТ-персонала. Эти изменения могут привести к появлению значительного числа новых типов уязвимостей, что создаст значительные трудности для сетевых проектировщиков и операторов. В «Плане стандартизации умных сетей МЭК» [5-1] подчёркивается, что кибербезопасность, в первую очередь, сыграет важную роль при создании эффективного и надёжного функционирования умных сетей. Требования по

кибербезопасности должны вытекать из оценки риска и общих архитектурных решений. Описание характеристик умных сетей [5-2] и вариантов применения мер безопасности является необходимой основой для данного вида работ, которые будут осуществляться непрерывно.

Фокусируясь на недостатках существующих стандартов кибербезопасности [5-3], данное рабочее направление в первую очередь дает характеристику, описывает категории и моделирование вредоносных киберугроз, что является ключевыми шагами в процессе оценки риска. Исходя из этого, разработка сосредотачивается на кибербезопасности умных приложений для топологий энергетических сетей, для которых характерно внедрение распределённых энергетических ресурсов с использованием возобновляемого источника энергии, устройствами хранения данных и регулируемыми нагрузками, а также с привлечением большого количества персонала к доменам умных сетей.

Чтобы проиллюстрировать это, будет рассмотрен характерный случай использования регулировки напряжения в активных распределительных сетях среднего уровня напряжения. Задача функции регулировки напряжения заключается в согласовании профиля напряжения на сетях среднего уровня напряжения для того, чтобы оптимизировать технические и экономические цели, отправляя заданные значения распределенным энергетическим ресурсам и распределительным сетевым устройствам.

Цель работы - продемонстрировать методы получения допустимых оценок сложности борьбы с различными видами кибератак для сервисов связи регулировки напряжения в рамках системы автоматизации подстанции.

Начиная с описания архитектуры регулировки напряжения как характерного способа использования будущих умных сетей, разработка сосредотачивается на применении языка моделирования кибербезопасности, предназначенного в данном случае для оценки пригодности устройств к умным сетям. Методика данного языка применяется для описания ИКТ архитектуры сетей (сетей, операционных систем, сервисов, протоколов, потоков данных и т.д.), мер безопасности, источников и целей атак. Подход с применением языка моделирования кибербезопасности обеспечивает допустимую количественную оценку вероятности того, что тот или иной способ атаки пройдёт успешно. В данной работе язык моделирования кибербезопасности будет использоваться для оценки вероятности определённой атаки, поражающей функции регулировки напряжения, включая атаки, вызванные процедурами дистанционного обслуживания на

устройствах регулировки напряжения.

В начале данной разработки (в главе 5.1) представлена схематическая модель, отображающая значение и связи между ключевыми понятиями рисков кибербезопасности. Далее в работе исследуется моделирование атак, решающее некоторые актуальные технические и архитектурные вопросы. В главе 5-2 объясняется, почему моделирование атак имеет решающее значение для оценки риска, а, впоследствии, в главе 5-3 представлены графические подходы к моделированию атаки. Во второй части работы продемонстрирована значимость моделирования атак умных сетей. В главе 5.4.1 представлена эталонная архитектура «Умных сетей» электроснабжения как основа для применения моделирования атаки, а в главах 5.4.2 и 5.4.3 рассматривается связь между моделированием атак и анализом безопасности с использованием деревьев атак и языка моделирования кибербезопасности. Окончание разработки представлено в главе 5.5, где подводятся итоги представленного материала и рассматриваются вопросы, которые всё ещё требуют решения.

5.1 Схематическая модель ключевых понятий риска кибербезопасности

Домены рисков кибербезопасности характеризуется использованием сложных и местами запутанных терминов и понятий. В доменах используются абстрактные и отвлечённые понятия, такие как угроза, риск, влияние, атака, уязвимость, эксплуатация, контрмера, вторжение, снижение риска, безопасность, доступность, целостность, конфиденциальность, неотрицаемость и т.д. Вышеперечисленные термины часто употребляются вместе с некоторыми более конкретными и значимыми понятиями, такими как «спуфинг» (используется хакерами для обхода систем управления доступом на основе IP-адресов путём маскирования под другую систему (её IP-адрес)), прослушивание сети, распределённый отказ в обслуживании атак, брандмауэр, система обнаружения вторжений, система предотвращения вторжений, вставки в программу (код для оперативного исправления или нейтрализации ошибки в исполняемой программе), внутренний нарушитель, взлом защиты, "фишинг" (преступная деятельность интернет-мошенников, действующих под видом благонадёжных компаний и юр. лиц, с целью незаконного получения секретной информации) и другие. Очень просто запутаться в такой смешанной терминологии. Хотя были предприняты попытки объединить их в общий справочник по безопасности, до сих пор не был создан единый унифицированный словарь. Вместо этого, некоторые из приведенных слов имеют изменяющиеся или даже

повторяющиеся значения, зависящие от контекста. Более того, между этими терминами может существовать неявная, неустановленная связь.

Схематические модели были предложены для того, чтобы попытаться отследить указанные взаимосвязи. Пожалуй, наиболее частому упоминанию подлежит та, которая принята согласно общим критериям (СС) ИСО/МЭК [5-4]. Связь между основными понятиями безопасности, предлагаемыми данной моделью, изображена на рис 5-1.

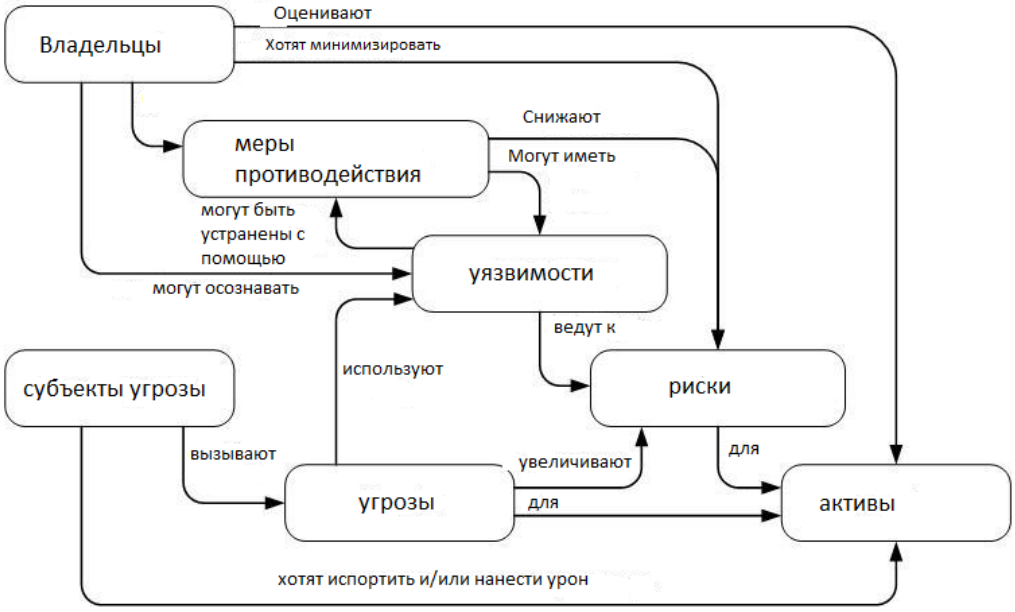

Рисунок 5-1 Концептуальная модель ключевых понятий риска кибербезопасности

Модель международного стандарта по компьютерной безопасности имеет некоторые недостатки. Она не является общепринятым словарём. Вместо этого она предлагает метод определения функциональных требований к безопасности и оценки гарантии их выполнения по градуированной шкале. Несмотря на это, модель международного стандарта по компьютерной безопасности набрала популярность благодаря её широкому применению. К примеру, данную схематическую модель можно использовать в вопросах кибербезопасности для энергетических систем. В этом случае «владельцами» являются компании генерации, распределения и передачи или другие действующие лица, такие как рынок и потребители. Термин «активы» может описывать основное оборудования и сам процесс (например, передача и распределение энергии). Аналогично, вторичное оборудование, такое как ИТ-инфраструктура и программное обеспечение тоже является «активом», даже если эти составляющие имеют явно меньшее значение для их владельцев. Модель международного стандарта по компьютерной безопасности разделяет понятия

«угрозы» и «субъекты угрозы». «Субъекты угрозы» - это любые потенциальные злоумышленники от хакеров-любителей до государств, создающих целенаправленные или нецеленаправленные угрозы. В отличие от этого, «угрозы» представляют собой потенциальные нарушения требований конфиденциальности, целостности и доступности различных активов. «Риск» - это сочетание вероятности совершения угрозы (каким-либо субъектом угрозы) и связанных с этим последствий. Наличие «уязвимостей» в системе, например, ошибок в исполнении наряду с нарушениями в конфигурации, позволяет в целом легче осуществить угрозу. Наконец, «контрмеры» - это любые функции, которые уменьшают уязвимости, тем самым снижая риск, включая ИТ-оборудование, обеспечивающее безопасность, такое как брандмауэры, системы предотвращения вторжений и неинформационные технологии, например, защита объекта по периметру или обучение персонала вопросам безопасности. Выяснилось, что модель международного стандарта по компьютерной безопасности является неполной, хоть и полезной. Прежде всего, она не предоставляет полного перечня понятий, связанных с безопасностью. Более того, хотя она и описывает взаимоотношения между разными понятиями, их причинно-следственные зависимости являются очень неявными. Например, можно узнать, что контрмеры снижают риск, но модель международного стандарта по компьютерной безопасности не указывает, какие конкретно меры устраняют тот или иной риск, а также их эффективность при данных обстоятельствах. Однако эти упущенные детали имеют решающее значение для осуществления оценки риска кибербезопасности в промышленных и практических условиях.

Альтернативная модель была разработана для того, чтобы устранить некоторые из этих недостатков, используя язык моделирования кибербезопасности[5-5], рис.5-2. Язык моделирования кибербезопасности - это определенный язык, метамодель, которая производит моделирование архитектуры информационных и коммуникационных технологий. Язык моделирования кибербезопасности находится на одной линии с моделью международного стандарта по компьютерной безопасности, но вдобавок предполагает явные причинно-следственные зависимости понятий, определенных вероятностным способом. Это достигается путем группировки терминов безопасности в формы либо явных «объектов», либо в качестве «свойств» этих объектов (так же, как в языках моделирования, таких как Унифицированный Язык Моделирования (UML)). Эти объекты связаны семантическими реальными отношениями, а свойства связаны с их причинно-следственными зависимостями. Язык моделирования кибербезопасности

сосредоточен вокруг «этапов атаки», которые нацелены на «критические кибер-активы». Существует некоторая вероятность для успешного проведения «этапов атаки», а «активы» обладают определенной стоимостью, «ожидаемым убытком» для «владельцев». Оценка владельца, таким образом, представляет его отношение к основному оборудованию, защищая которое он тратит кибер-активы. Продукт этой оценки и вероятность того, что атака принесёт ожидаемый убыток, соответствуют общепринятой концепции риска. Различие, которое существует между языком моделирования кибербезопасности и моделью международного стандарта по компьютерной безопасности заключается в способах описания «угрозы». Согласно языку моделирования кибербезопасности «угроза» - это определенный сценарий атаки, состоящий из набора «этапов атаки». «Угрозы» распространяются субъектами атаки. Важно, что «этапы атаки» включают в себя вероятностные измерения. «Угроза» указывает на вероятность того, что набор ходов атаки выбран успешно, если данные этапы были пройдены. Все единичные вероятности поэтапной атаки основываются на сочетании знаний, полученных от экспертов в данной области и опубликованных ранее академических научных исследований. «Атакующий» рассматривается как профессиональный испытатель, обладающий одной неделей для подготовки к «вторжению». Наконец, «этапы атаки» могут быть более-менее эффективно урегулированы с помощью «контрмер». Определение, используемое для описания «контрмер»: это вторая ключевая особенность языка моделирования кибербезопасности. «контрмеры» - это особый вид «активов», который предназначен для защиты других «активов». Язык моделирования кибербезопасности различает пять типов контрмер:

- Восстановительная - запускается только после того, как атака совершена (например, резервное копирование);
- Превентивная - усложняет проведение атаки (например, брандмауэры и контроль доступом);
- Выявляющая - исключительно регистрирует атаки и включает сигналы тревоги (например, системы обнаружения вторжений);
- Реагирующая - является комбинацией выявляющих и превентивных контрмер и обладает достаточными возможностями, чтобы активно принимать меры предосторожности в условиях атаки;
- Контролирующая - не смягчает последствия атаки, а собирает информацию о ней. Это окажет сильное влияние на успех проведения, благодаря которому стоит

ожидать, что хорошая контролируемая защита отпугнет «атакующих», которые хотят минимизировать риск на их поимку.

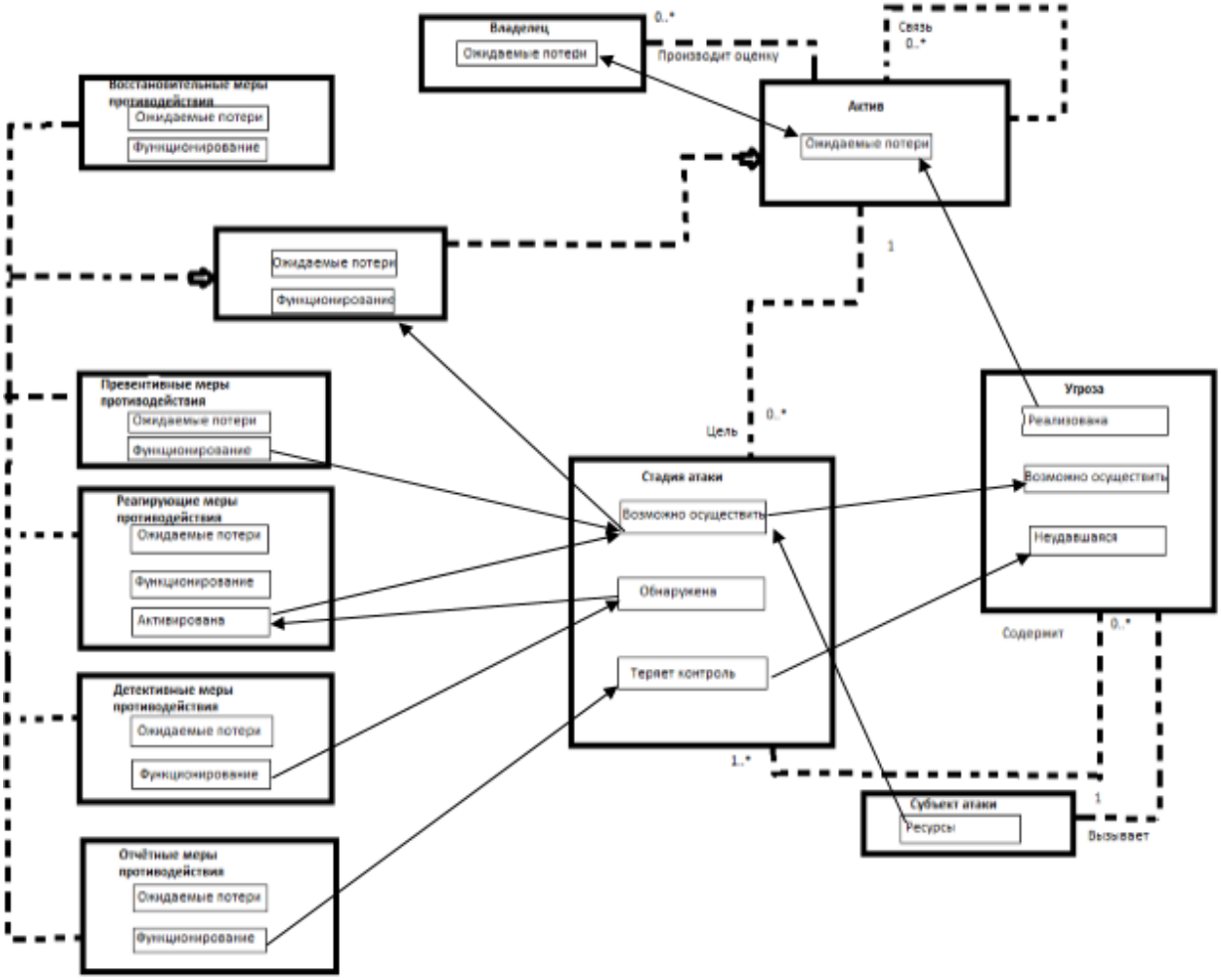

Рисунок 5-2 Приложение CySeMoL

Из рассуждения, представленных выше, становится ясно, что язык моделирования кибербезопасности представляет собой пример эталонной модели, которая пытается установить более строгую терминологию для взаимодействия, моделирования и анализа кибербезопасности. Как и было сказано, данная модель сохранит свою актуальность в краткосрочной перспективе, чтобы определить чёткую концептуальную основу для каждой рабочей среды. По мере того, как эта глава нацелена на пояснение процессов атаки, необходимо привести подобные объяснения другим понятиям.

5.2 Почему моделирование атаки является основой задачей при оценке риска

Ключевой целью для оператора электрических сетей является снижение влияния угроз на непрерывную поставку электроэнергии. Угрозы для управления электрическими сетями

включают в себя погодные условия, такие как шторм или сильный снегопад, отказ основного оборудования из-за растущей зависимости от информационно-коммуникационных технологий (ИКТ), а также отказ другого оборудования, например, ошибки в программном обеспечении или сбой коммуникационного оборудования. Особые виды угроз, часто классифицируемые как риски в обеспечении безопасности - это враждебные угрозы, например, вандализм, терроризм или даже военные действия. Предупреждение об инцидент с вирусом Stuxnet в 2010 году неоспоримо продемонстрировао целесообразность антагонистических угроз, возникших из кибер-доменов промышленных систем управления. Это подчёркивает важность учета кибер-угроз в процессах анализа значительного риска, а также в процессах управления энергетических предприятий. Независимо от используемой схематической инфраструктуры, понятие риска кибербезопасности, как правило, разделяется на два направления, которые включают в себя оценки последствий умышленных угроз и оценки вероятностей реализации угрозы. Оценка последствий зачастую не вызывает затруднений, а сами последствия часто переводятся в денежную стоимость (хотя исходы, не поддающиеся оценке, такие как смерть или потеря доверия в организации, также могут быть рассмотрены в рамках целостного подхода к риску). Оценка вероятности реализации угрозы - это более сложный процесс, зависящий как от вероятности того, что атака пройдёт успешно, так и от вероятности того, будет совершена попытка атаки. С другой стороны, эти элементы зависят как от свойств «атакующего», так и от свойств ИКТ-инфраструктуры.

Приведенная зависимость довольно важна. Она выдвигает на первый план то, что может быть проконтролировано лицами, принимающими решения в области кибербезопасности при помощи выбора ИКТ-инфраструктуры. Например, последствия атак зависят, прежде всего, от условий эксплуатации, определённых работой оборудования, хотя они и подвергающиеся влиянию контрмер ИКТ-инфраструктуры. Более того, навыки и поведение субъектов атаки с точки зрения лиц, принимающих решения относительно кибербезопасности поддаются наблюдению, но не контролируются. Однако вероятность реализации атаки может подвергаться отбору ИКТ-инфраструктуры. Таким образом, вполне естественно, что любая методология или инструмент принятия решений сфокусированы на данном понятии. Независимо от того, является ли ответственный за принятие решений оператором системы передачи энергии, действующей в стране, оказавшейся перед угрозой войны, или оператором распределительной системы в

обществе с низким уровнем преступности - процесс принятия решения часто фокусируется на том, сколько контрмер необходимо предпринять для уменьшения вероятности реализации угрозы.

К сожалению, понятие зависимости между разнообразными типами атак и контрмер в различных ИКТ-инфраструктурах недостаточно освещено в многочисленных стандартах и документах, удовлетворяющих требованиям. Приближенно, они могут быть приведены в качестве списка отдельно взятых рекомендуемых норм.

Ключ к тому, чтобы понять, как оптимизировать безопасность ИКТ-инфраструктуры заключается в понимании различных уязвимостей системы в целом. Эффективный подход к данной проблеме является моделирование и исследование различных сценариев атаки системы. По существу, сценарии атаки – это этапы действий, которые «атакующему» необходимо предпринять, чтобы ясно представлять себе угрозу. Их описание может быть, как текстовым, так и графическим. Первоначально, графическое моделирование атаки сфокусировано исключительно на технических вопросах. С тех пор данные методы были расширены и стали включать в себя более «мягкие» организационные аспекты, так как безопасность является свойством системного уровня. Например, технически усовершенствованное решение в области управления доступом отвергается, если кто-либо может позвонить в службу поддержки и получить информацию об отчёте. В следующей главе мы рассмотрим методы графического представления и сравнения сценариев атаки.

5.3 Обзор методов графического моделирования атак

Системы графического моделирования атаки включают визуальное представление различных сценариев, которым атака может следовать, чтобы прийти к цели, обеспечивая, таким образом, анализ сценариев. Деревья атак могут соответствовать тактике «атакующего», системы/организации, находящихся под атакой или на нейтральной стороне. Оборонительные аспекты также могут быть объединены, чтобы оценить эффективность контрмер. Рассмотрение модели может быть исключительно качественным, но, кроме того, относиться к количественным аспектам.

Существует множество систем графического моделирования атаки. Наиболее известным и широко-используемым является метод дерева атак[5-7]. Ориентируясь на систему дерева неисправностей, часто используемую для гарантии безопасности, стадии и техники атаки объединены в булевом логическом дереве, с целью атаки «конечным событием» (корнем)-

рис.5.3. Деревья атак применяются к целому ряду различных систем, включая системы, относящиеся к блокам электропитания, такие как система диспетчерского управления и сбора данных (SCADA) [5-8][5-9], умные измерительные системы[5-10] или автоматика безопасности в ядерных энергоустановках[5-11].

Дополняя деревья атак, существует несколько более научных систем моделирования атак. Они включают в себя принципы, основанные на сетях Петри[5-12][5-13], Байсовских сетях (см. [5-14] пример для системы SCADA) или ориентированные на унифицированный язык моделирования(UML), например, случаи нарушения[5-15] и неверного использования[5-16].

Каждый из доступных методов предлагает выбор оптимального соотношения между считываемостью, масштабируемостью, моделированием мощности и количественной оценкой возможностей. Например, деревья атак просты в чтении, но, являясь нединамичными системами, они недостаточно действенны. С другой стороны, подходы, основанные на сетях Петри, очень действенные, но с ними сложно справиться не обученным в данной сфере людям.

Учитывая такие различия, неудивительно, что каждый из авторов рассматривал конкретные индивидуальные методы. Например, в исследовании энергетических систем (RSE) применяются диаграммы состояний для подходов моделирования атак[5-17], изображённые на рис.5-4, которые можно увидеть, как горизонтальное расширение упорядоченного дерева целей с временными переходами. В качестве альтернативы, научно-исследовательский отдел компании Électricité de France (EDF), разработал систему под названием BDMP (булево логическое дерево Марковского процесса) [5-19], которая визуально близка к деревьям атак и, кроме того, обеспечивает моделирование динамических параметров, таких как порядок этапов атаки, обнаружения и реакции. На рис. 5-5 приведен пример данной системы. Система была заимствована из области надёжности[5-20], она содержит различные толкования, которых нет в классических деревьях атак. В заключение, Королевский Технологический Институт разработал вероятностную модель для анализа кибер-риска [5-5], показанную на рис.5-2, которая предоставляет возможность изображать стадии атаки, предлагая более широкий инструментарий, поддерживающий вычисление рисков в UML-подобной диаграмме классов.

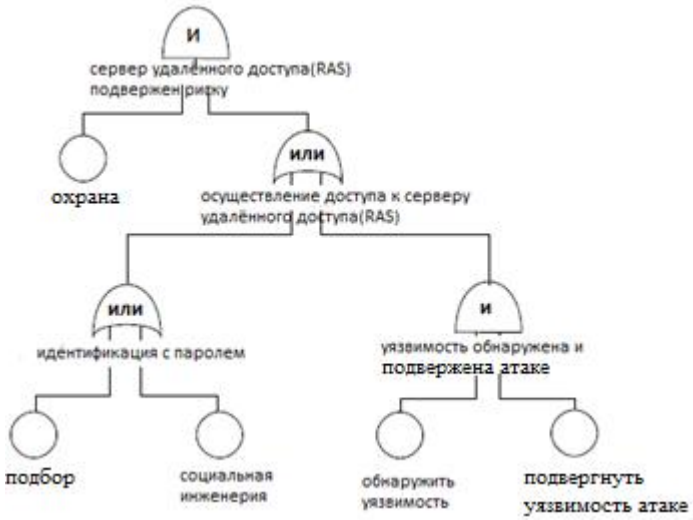

Рисунок 5-3 Дерево атак на коммутируемом сервере удалённого доступа (RAS)

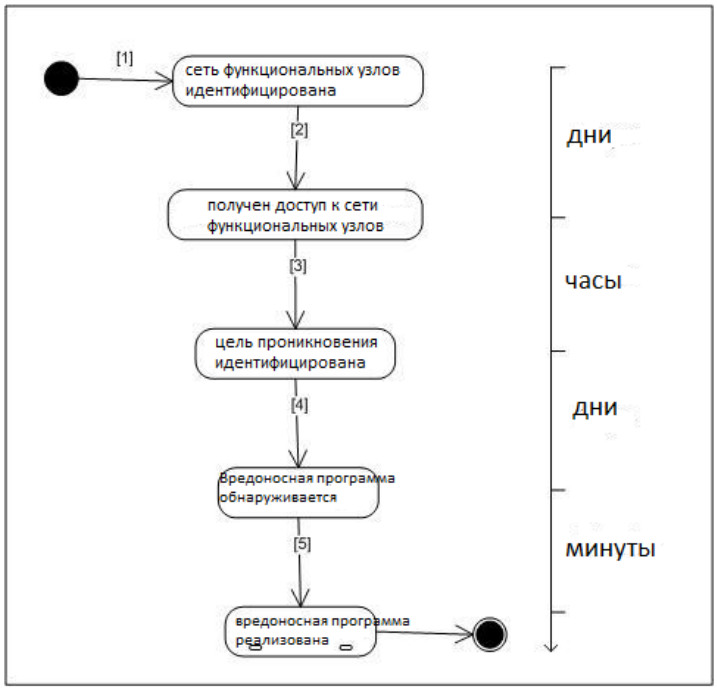

Рисунок 5-4 Характерная диаграмма состояния атака RSE

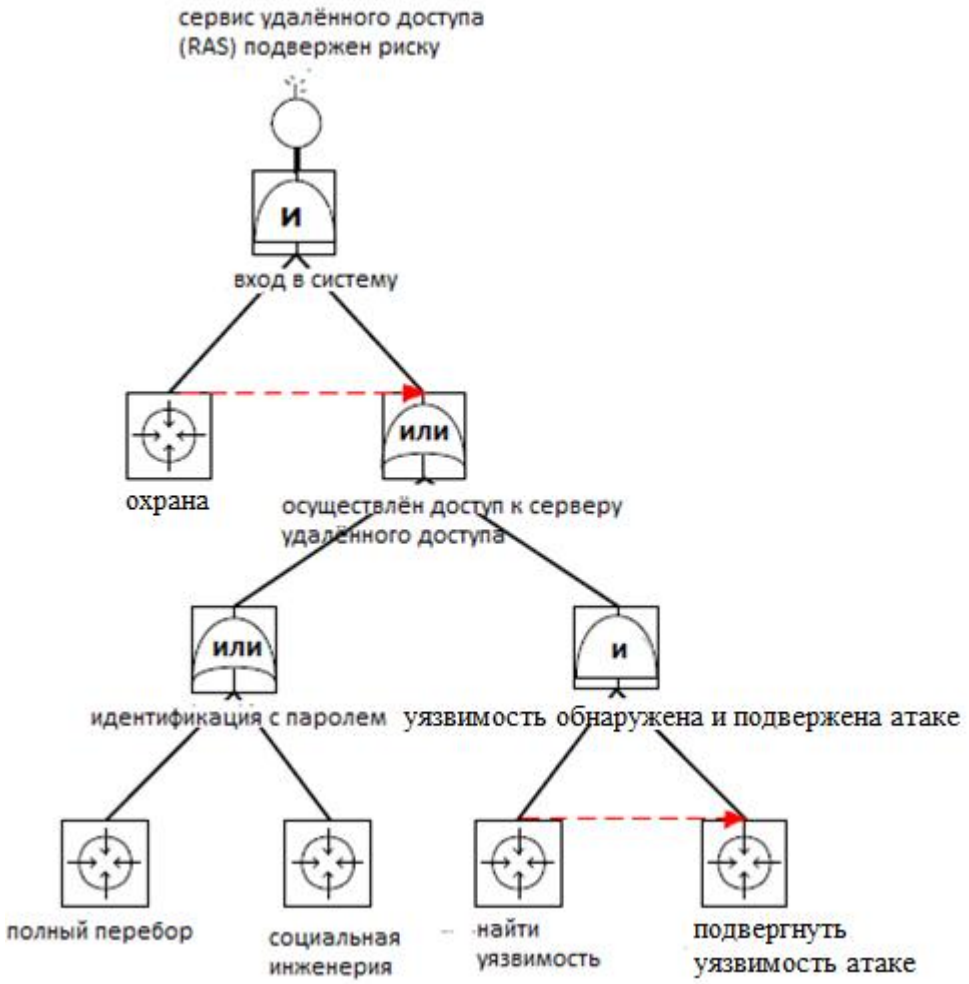

Рисунок 5-5 BDMP-моделирование атаки сервера удалённого доступа (RAS) (в последовательности, указанной красными стрелками)

Для качественных оценок, обычный процесс использования метода графического моделирования позволяет упростить определение вероятности, которое может быть основано на реальных и визуальных представлениях. Дискуссии и дебаты среди экспертов возникают все реже, а разнообразие возможных путей атаки является более ясным и понятным. Для дополнительных количественных анализов к моделям могут быть добавлены различные числовые параметры, включая вероятностные, зависящие от выбранной техники моделирования атаки. В целом, моделирование атак также может помочь в дальнейших процессах оценки рисков и в выявлении уязвимой части архитектуры безопасности и организации в целом: Определенные стадии и техники атаки могут проявиться во многих сценариях, а также для разных целей злоумышленников, указывая на необходимый недостаток, который нужно устранить. Автоматическая обработка модели может в некотором случае помочь аналитику в этой задаче, в

зависимости от выбранного метода моделирования.

В дополнение к предыдущим рассуждениям, доступны более подробные примеры использования деревьев атаки. Некоторые методы (в основном из США) подробно описывают использование деревьев атаки в процессе оценки риска. Конкретные примеры включают в себя требования качества безопасности к проектированию (SQUARE), разработанные университетом Карнеги Меллон [5-21] или методика риск - ориентированного анализа (MORDA), разработанная Агенством Национальной Безопасности США и в основном используемая в оборонной промышленности. [5-22] [5-23]. Подходя к области, больше связанной с блоками электропитания, в справочнике по кибербезопасности АЭС также упоминается использование деревьев атаки в анализах риска [5-24].

Во-первых, система деревьев атаки будет использоваться, чтобы изобразить сценарий атаки на эталонную архитектуру функций регулировки напряжения, описанную в главе 5.4. Такой выбор был сделан не для гипотетического превосходства в отношении других систем. Все это потому, что деревья атаки обеспечивают наиболее понятное и доступное представление в контексте данной работы. Во-вторых, использование языка моделирования — кибербезопасности - это представление с указанием вида оценки, лежащее в основе метода моделирования.

5.4 Анализ безопасности контроля напряжения в активных распределительных сетях

5.4.1 Эталонная архитектура

Работа активных распределительных сетей с большим потоком распределенных энергоресурсов (РЭР), подключенных к линиям среднего напряжения (СН), требует внедрения новой функции контроля напряжения (ср. случай РГПД-0200 в [5-25]). В линиях СН, включая распределение выработанной энергии, мощность, полученная с помощью РЭР, может привести к превышению допустимых значений напряжения в некоторых частях сети, в основном, вследствие неконтролируемого вырабатывания энергии из возобновляемых источников. Управляющие воздействия, ограничиваемые переключателями ответвлений на линиях (ПОНЛ) у трансформаторов на подстанциях и компенсационными мерами, как обычно происходит в пассивных сетях, могут оказаться недостаточными, чтобы ответить требованиям снабжения, установленным нормой EN

50160. Профили напряжения в СН сетях также могут быть настроены с помощью влияния на РЭР, подведенных к линиям СН и устройствами на подстанциях, такими как конденсаторные батареи и другими накопителями энергии.

На рисунке 5-6 представлены основные компоненты архитектуры контроля сетки, включенные в функцию контроля напряжения (КН). Сосредотачивая внимание на подстанции высокого напряжения (ВН)/СН, рисунок указывает на необходимость новой функции КН, выполненной с помощью системы контроля на уровне станции (называемой НКСД на подстанции). Главный контур контроля функции КН основан на подстанции - центре, внутренней подстанции и линиях поставки РЭР на подстанции. С учетом топологии сети, полевых измерений, рыночных цен и затрат на эксплуатацию ресурсов, функция КН оптимизирует профиль напряжения, вычисляя и посылая соответствующие установки третьей стороне, занимающейся распределенными энергетическими ресурсами (генераторы, переменные нагрузки и накопители энергии) и устройствам распределения (т.е. батареям конденсаторов и ПОНЛ). Алгоритм основан на оптимальной мощности потока постоянного тока, где потери в сети и интегральная напряженность принимаются во внимание. Статус сети, запрашиваемый алгоритмом контроля, вычисляется функцией состояния оценки, основанной на реальных измерениях и топологии сети.

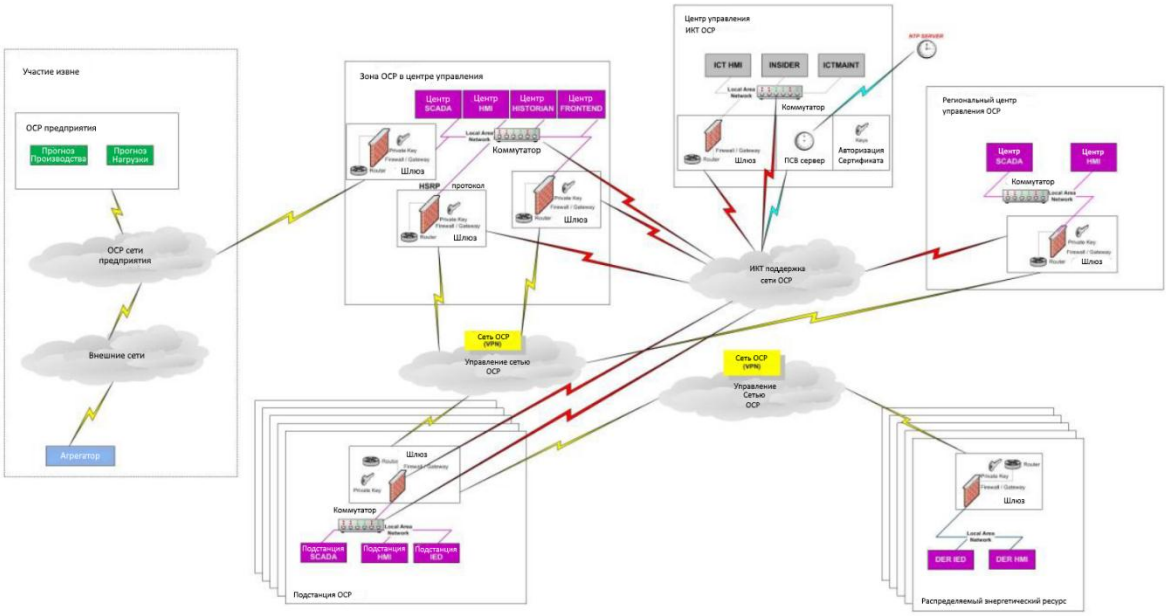

Рисунок 5-6 ИКТ архитектура функции контроля напряжения

Руководство и управление безопасностью центра и компонентов ИКТ подстанции и компьютерной сети выполняются ОСР ИКТ центра управления. Он имеет прямой доступ

к сети и компонентам управления, за исключением элементов ИЭУ на подстанции и компонентов РЭР. Потоки данных для удаленного управления связью и устройствами контроля основаны на использовании защищенных операций, например, протоколы HTTPS и SSH.

В соответствии с архитектурной планировкой на рисунке 5-6, цепь поставок функции КН зависит от нескольких связных звеньев с участием удаленных доступов из систем, находящихся вне зоны контроля ОСР. В частности, приложение КН на подстанциях имеет линии связи с третьей стороной РЭР, возможно развертывание разного рода технологий связи, доступных в различных географических районах. С исходной точки работы, функция оптимизации должна получать запросы регулирования напряжения от ОСП (оператора системы передачи) всякий раз, когда относительно сети передачи в случае непредвиденных обстоятельств необходимо применять предупредительные меры при аварийных значениях напряжения. Прогнозы загрузки и генерации используются для оптимизации работы распределенных устройств, в то время как экономическая оптимизация основывается на рыночных ценах и затратах на эксплуатацию РЭР.

Обмен информацией функции КН может быть отображен в протоколе МЭК 60870-5-104 (для связи с центральной подстанцией) и в профиле MMS по стандарту МЭК 61850 (для внутренней подстанции и линий поставки РЭР на подстанции).

Сосредоточив внимание на основе схемы регулирования СН, станет очевидно, что правильная разработка оптимальных установок зависит от предоставления правильных эксплуатационных и экономических данных из вышеуказанных каналов связи [5-26]. Вредоносная атака одного из вышеуказанных звеньев связи может привести к потере прогнозов выработки энергии, рыночных экономических данных, запросов от ОСП, а также к изменениям топологии сети, утере рабочих данных из СУД, введению ложных прогнозов выработки энергии, рыночных экономических данных, запросов от ОСП, топологических изменений, оперативных данных из СУД, данных мониторинга или установок. Последствия атак связи могут привести функцию регулирования либо к отклонению от оптимальных установок или, что еще хуже, к созданию неверных установок с каскадными последствиями на подключенные генераторы. Цель контрмер безопасности, интегрированная в архитектуру, заключается в обеспечении доступности и целостности требований связи, т.е. в восполнении потерь данных и в предотвращении введения ложных сообщений.

5.4.2 Пример «дерева атаки»

Типичный анализ рисков кибербезопасности требует идентификации и иерархизации критических функций, и защиты связанных с ними вспомогательных систем. Такие результаты учитывают, как потенциальные последствия, так и вероятность нарушения работы функций и связанных с ними систем. Предыдущая работа рабочей группы СИГРЭ D2.22 уже описала и рассмотрела различные методологии анализа риска, ссылка [5-27], в то время как общие критерии можно найти в стандарте ИСО / МЭК 27005 на тему точки зрения информационной безопасности [5-28]. Что касается случаев использования «Умных сетей», представленных ранее, предполагается, что процесс предварительного анализа риска привел нас к сосредоточению на автоматизации подстанций и, в частности, на правильности функции уровня отсека КН.

Роль функции КН заключается в настройке профиля напряжения в сети СН для оптимизации указанных технических и экономических задач, посылая соответствующие команды распределенным энергоресурсам и устройствам распределения энергосистемы (например, конденсаторным батареям, ПОНЛ выключателям, линиям СН). Требуется несколько информационных потоков, состоящих из обмена топологией энергосистемы, полевых измерений и рыночных цен. Ограниченные измерения, полученные из поля, означают, что существует необходимость завершить фактические измерения с помощью результатов измерений, вычисленных функцией состояния оценки. Эта функция также учитывает прогнозы распределенного производства энергии и потребление ее интеллектуальными нагрузками. В предполагаемой архитектуре принимается, что прогнозы выработки энергии будут предоставлены внешней системой, сообщающейся с центральной СУД, в то время как прогнозы нагрузки являются функцией, обеспечиваемой самой СУД. И, наконец, оператор системы передачи также может посылать сигналы системе КН в целях осуществления мер защиты, касающихся общей стабильности связанной сети.

На следующем рисунке 5-7 представлен общий вид ввода/вывода функции КН. Этот рисунок является дополнительным и согласуется с архитектурной схемой, показанной на рисунке 5-6. Информационные потоки были упрощены для содействия разработке модели атаки.

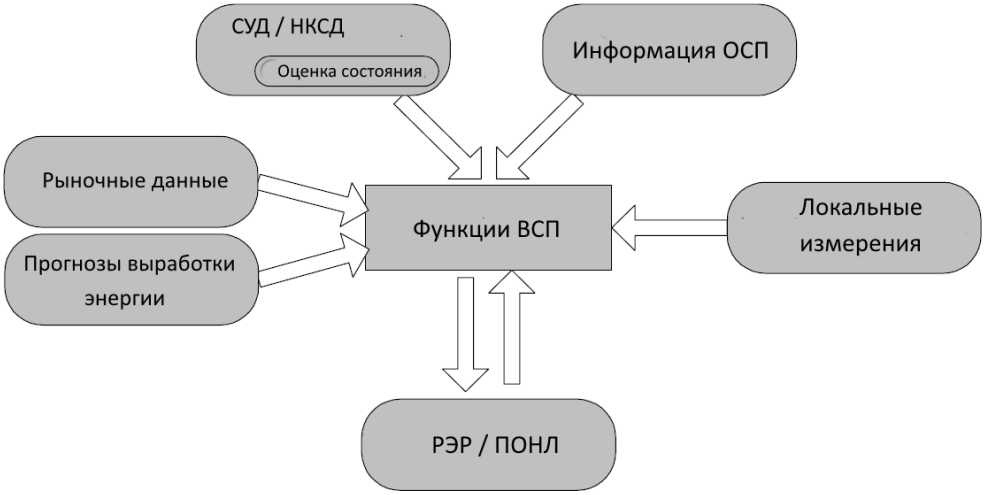

Рисунок 5-7 Общий вид ввода/вывода функции контроля напряжения

Рассмотрим теперь характеристику вероятности атак на такую функцию. В этом процессе, графические методы моделирования атаки, подобные методам, описанным в разделе 5.3, могут обеспечить ценную поддержку. С качественной точки зрения это достигается путем увеличения зоны действия анализа в отношении сценариев и методов нападения, а также выяснением потенциальных уязвимостей, принимаемых во внимание. В зависимости от выбранного метода, количественный анализ также может дополнять и помогать процессу оценки вероятности для сравнения и классификации вероятностей других сценариев, в общем анализе риска. Начиная от общего представления ввода/вывода функции КН на рисунке 5-7, сценарии атак, приводящие к неправильным результатам функции КН, могут быть сгруппированы в три категории, каждая из которых будет отражена в графической модели атаки. Сценарии атаки включают в себя:

• атаки при вводе функций КН, либо в самом источнике или сообщениях;

• атаки на систему, обрабатывающую функцию;

• атаки при выводе функции.

Рис. 5-8 дает представление дерева атаки высокого уровня после такой аварии. Ветви верхнего уровня и выводы соответствуют категориям высокого уровня атак, ранее описанным, плюс учет выводов для атак законных удаленных объектов. Подробные поддеревья должны быть разработаны и подключены к этой структуре, с тем, чтобы представлять конкретные методы атаки и использование уязвимости. Эти более низкие уровни разложения требуют видения инфраструктуры связи, такой, как показано на

рисунке 5-6. Рисунок 5-8 представляет некоторые начальные стадии разложения процесса атаки, приводящие к онлайн искажению необходимых вводных сообщений функции КН. Под логическим элементом «ИЛИ» "модификации входных сообщений", Рисунок 5-8 подразумевает возможный подход к искажению информации, посланной ОСП. Такие ориентированные на сеть атаки могут включать конкретные подмену и подделку методов, а также получение доступа к фактическим каналам связи. В качестве альтернативы, процесс вторжения может быть использован для атаки системы, обрабатывающей функцию. Процесс проникновения, в свою очередь, может быть разбит на промежуточные этапы, такие как: нарушение локального доступа к контролю измерения, перехват, а затем использование удаленных полномочий доступа и, наконец, искажение процесса. Как показано на рисунке, моделирование конкретных атак требует больших технических компонентов архитектуры связи (ср. рисунок 5-6). В любом случае, иерархический характер обозначений булевого дерева делает возможным различную глубину представления этих элементов. Более того, если динамические аспекты атак (т.е. порядок и сроки различных этапов атаки) считаются важными, простое представление дерева атака может быть замещено с помощью динамических методов моделирования (ср. раздел 5.3).

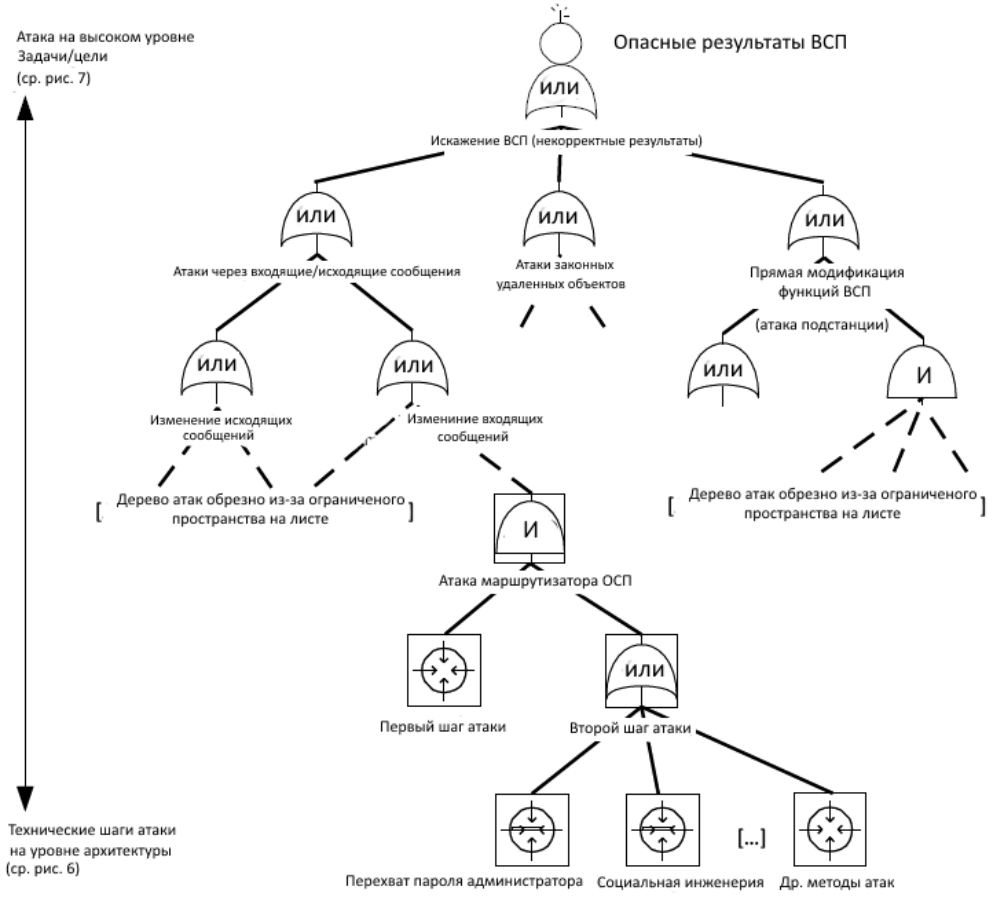

Рисунок 5-8 Фрагмент дерева атаки

5.4.3 Архитектура контроля напряжения на языке CySeMoL

Основные понятия, смоделированные на CySeMoL, следующие. Во-первых, каждая локальная сеть (например, центр контроля над областью ОСР) моделируется как сетевая зона, при условии полной достижимости между произвольными узлами (например, сервисами, приложениями или операционными системами), расположенными в пределах сетевой зоны. Сетевые зоны соединены между собой через шлюзы, с помощью которых межсетевые экраны и системы обнаружения вторжений могут быть связаны. Во-вторых, в рамках каждой из сетевых зон и между ними существуют сервисы, приложения и операционные системы (т.е. установленное программное обеспечение), каждое из которых соответствует программному продукту. В-третьих, услуги, приложения и другие установки программного обеспечения могут подключаться и взаимодействовать друг с другом. Это моделируется с помощью потоков данных и протоколов, в то время как управление данными моделируется хранилищами данных. В-четвертых, есть люди-пользователи, имеющие доступ к системам, которые могут быть защищены с помощью идентификации - точек контроля доступа, механизмов идентификации и учетных записей пользователей. В заключение, сетевые зоны могут быть связаны с физическими зонами и процессами управления зонами. Для более подробного описания языка CySeMoL, см. [5-29]. CySeMoL вместе с соответствующим программным средством может быть скачан[8] онлайн.

Для того чтобы уменьшить объем анализа, эта работа охватывает Центр Контроля над Областью ОСР, Подстанцию ОСР, РЭР и Центр Контроля ОСР ИКТ, вместе с их взаимосвязями и связанными информационными потоками. Что касается мер безопасности, возможности межсетевых экранов во взаимосвязанных шлюзах, шлюз-шлюз сетевом уровне ВЧС и непрерывном транспортном уровне безопасности, как это предписано в 3 части стандарта МЭК 62351 [5-30], сравнительно оценены с помощью запуска CySeMoL.

Что касается сценариев атаки, эта работа фокусируется на процессах атаки, пользующихся уязвимостью удаленных доступов к обслуживанию ИКТ на подстанции НКСД, и ориентированных на генерацию поддельных установок. Программное средство будет оценивать вероятность успеха возможных атак, сортируя их путем уменьшения

[8] http://www.ics.kth.se/cysemol

вероятности. Более подробное описание Уязвимости / действия, использованные / осуществленные в процессе атаки, получившие самые высокие баллы, будут затем рассмотрены для дальнейшей защиты от остаточных рисков.

Архитектура ИКТ при оценке разделяется на четыре логические зоны: центр контроля ОСР ИКТ; центр контроля над областью ОСР; подстанции ОСР; и РЭР (см. рисунок 5-9). Каждая из этих логических зон соответствует сетевой зоне (локальная сеть) и физической зоне в CySeMoL.

Мы моделируем и оцениваем три варианта реализации механизма обмена данными подстанции, кратко изображенных на рисунке 5-2. Во всех вариантах, имеется единственный шлюз в каждой подстанции, который соединяет локальную сеть подстанции (LAN) со всеми другими непосредственными сетями. Варианты отличаются использованием различной конфигурации ВЧС для защиты связи. Они описаны в следующем разделе.

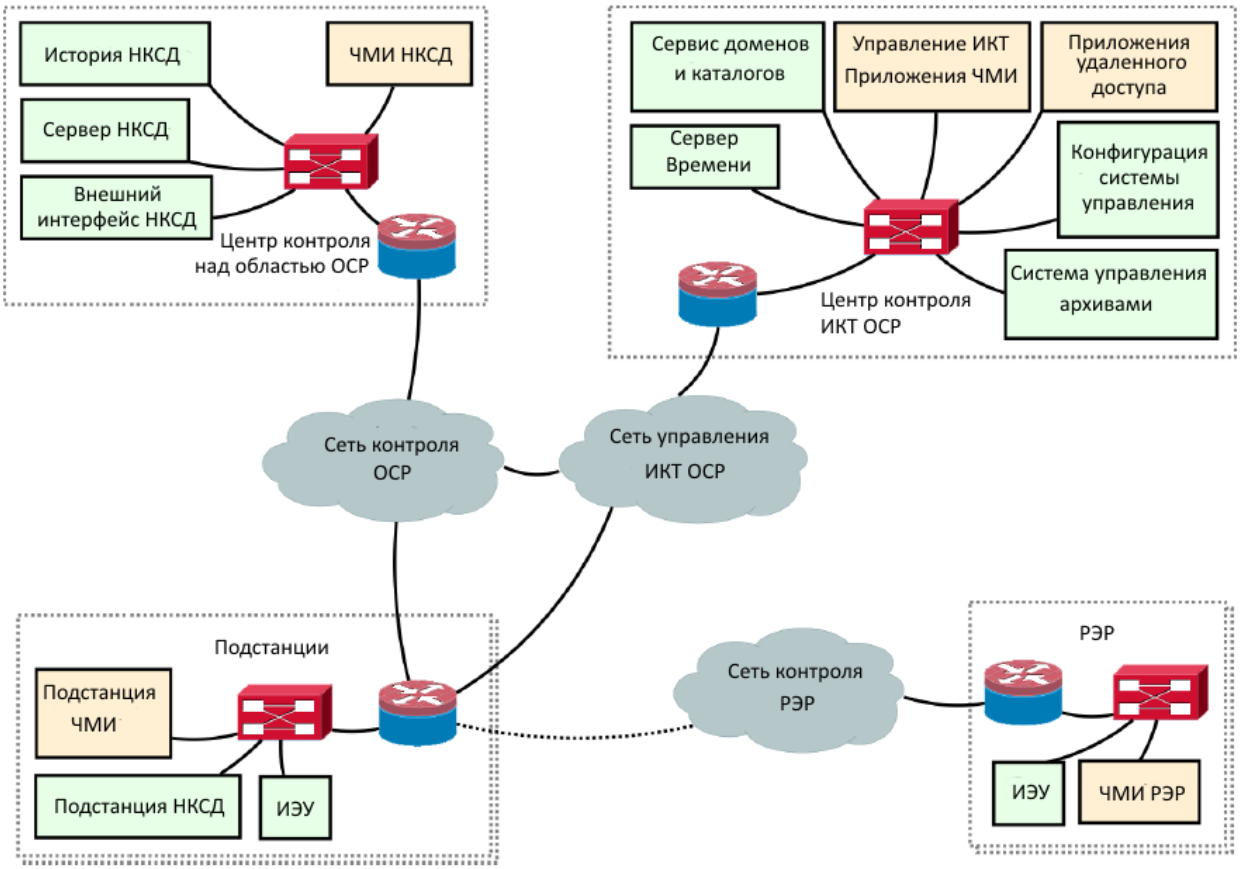

Рисунок 5-9 Сервисы и приложения в ИКТ архитектуре

Из центра контроля ОСР ИКТ технические специалисты ИКТ поддерживают

инфраструктуру ОСР ИКТ. Центр также руководит несколькими услугами, которые поддерживают инфраструктуру ИКТ и ее деятельность. Поэтому мы предполагаем, что центр заведует следующими системами: (1) система управления архивами; (2) сервер времени; (3) сервис каталога домена; и (4) сервер управления конфигурацией и обновлением. Кроме того, приложения для удаленного доступа и технического обслуживания используются из центра. Центр контроля над областью ОСР, из которого ведутся управление и наблюдение за энергосистемой, руководит системой НКСД и ее компонентами: сервером НКСД; историком; внешним интерфейсом; а также интерфейсом «человек-машина» (ЧМИ). На каждой из подстанций есть локальный сервис НКСД, интеллектуальные электронные устройства (ИЭУ), а также локальный ЧМИ (для целей технического обслуживания). На каждом из РЭР есть ИЭУ и локальный ЧМИ. Каждый из центров подключается к соответствующим внешним сетям через шлюз с межсетевым экраном. Рисунок 5-9 представляет обзор архитектуры ИКТ в отношении сервисов и приложений, запускающихся в/из соответствующих сетей. Каждая из систем моделируется как состоящая из сервиса или приложения-клиента и операционной системы, на которой она работает. Они подключены к соответствующим сетевым зонам.

Упомянутые выше системы соединены между собой и взаимодействуют даже через соответствующие сетевые зоны. Поэтому мы моделируем потоки данных и соответствующие протоколы следующим образом. Временная синхронизация осуществляется с использованием протокола сетевого времени (ПСВ). Все операционные системы используется в пределах периода времени, когда ОСР действует синхронно с сервером времени, помещенным в центре управления ОСР ИКТ. Сервер времени, также, как и операционные системы в РЭР, синхронизируется непосредственно с источником Интернета. Сервис каталогов используется для разрешения имен хостов и контроля доступа в пределах домена ОСР. Взаимосвязанные приложения, сервисы и лежащие в их основе операционные системы используют сервисы каталогов из всех сетей ОСР (таким образом, исключая РЭР). Используемый набор протоколов – X.500. Автоматизация процессов происходит между подстанциями и РЭР (ИЭУ РЭР или подстанцией НКСД), в пределах подстанций (подстанцией ИЭУ или подстанцией НКСД), между подстанциями и центром контроля над областью ОСР (подстанцией НКСД или внешним интерфейсом контрольного центра НКСД), а также в центре контроля над областью ОСР (сервере НКСД или внешнем интерфейсе НКСД, историке и ЧМИ). Для образования связи на внутренней подстанции и между подстанциями и РЭР используется стандарт МЭК 61850

(MMS и профили УООСП). Центральная система НКСД взаимодействует с НКСД уровня подстанции с использованием протокола МЭК 60870-5-104. Техническое обслуживание процессов на подстанциях осуществляется операторами из центра контроля над областью ОСР, а также техническим персоналом непосредственно на подстанциях. Первое осуществляется через центральную НКСД, и при этом используется протокол МЭК 60870-5-104. Второе осуществляется через ЧМИ на подстанции, который обменивается данными с НКСД подстанции. Обслуживание ИКТ осуществляется администраторами ИКТ в центре контроля ОСР ИКТ. Администраторы могут войти в произвольную операционную систему, оснащенную службой удаленного доступа. Удаленный доступ осуществляется с помощью протокола SSH и SSH-туннелированного протокола виртуальной сети. Операции обновления выполняются через сервер обновления и настроек управления, к которому подключено большинство операционных систем ОСР. Хотя некоторые системы настроены на автоматическое обновление (например, рабочие станции и некоторые серверы управления ИКТ), в то время как другие системы нуждаются в административном вмешательстве (например, серверы, управляющие услугами слежения за процессами), все системы загружают списки обновлений и обновления с сервера обновлений, используя либо Microsoft Windows Update (протокол MS-WUSP), или HTTPS доступ для обновления списков и пакетов обновления (в системах Linux). И, наконец, ЧМИ НКСД и в центре контроля над областью ОСР, и на подстанциях взаимодействуют с системой управления архивами, расположенной в центре контроля ОСР ИКТ, при необходимости беспрепятственно предоставляя информацию о продукте для операторов и техников. При таком взаимодействии используются веб-службы, основанные на протоколе HTTPS.

Говоря о доступе и идентификации, мы предполагаем, что есть три типа пользователей – оператор (оператор системы распределения в центре управления), технический специалист (на уровне подстанции) и ИКТ-администратор (оператор системы распределения в центре управления ИКТ). Банковские реквизиты и учетные данные для доступа к ним сохранены в домене службы каталогов, а также в компьютерах на локальном уровне, который они используют, где обычно происходит аутентификация (обнаружение подлинности).

Все части ИКТ-архитектур, описанные выше, были смоделированы на языке CySeMoL. Часть общей модели на языке CySeMoL представлена на рисунке 5-10.

Для того, чтобы смоделировать конфигурацию и свойства ИКТ-архитектуры, мы вынесли многочисленные предложения и попытались отразить типичные конфигурации сетей, протоколов и систем. Для большинства смоделированных объектов, упомянутых выше (например, сервисы, операционные системы, шлюзы, зональные управленческие процессы и т.д.), существует множество параметров, на основании которых язык CySeMoL также оценивает тенденцию кибербезопасности. Наши предположения кратко описаны в таблице 5-1.

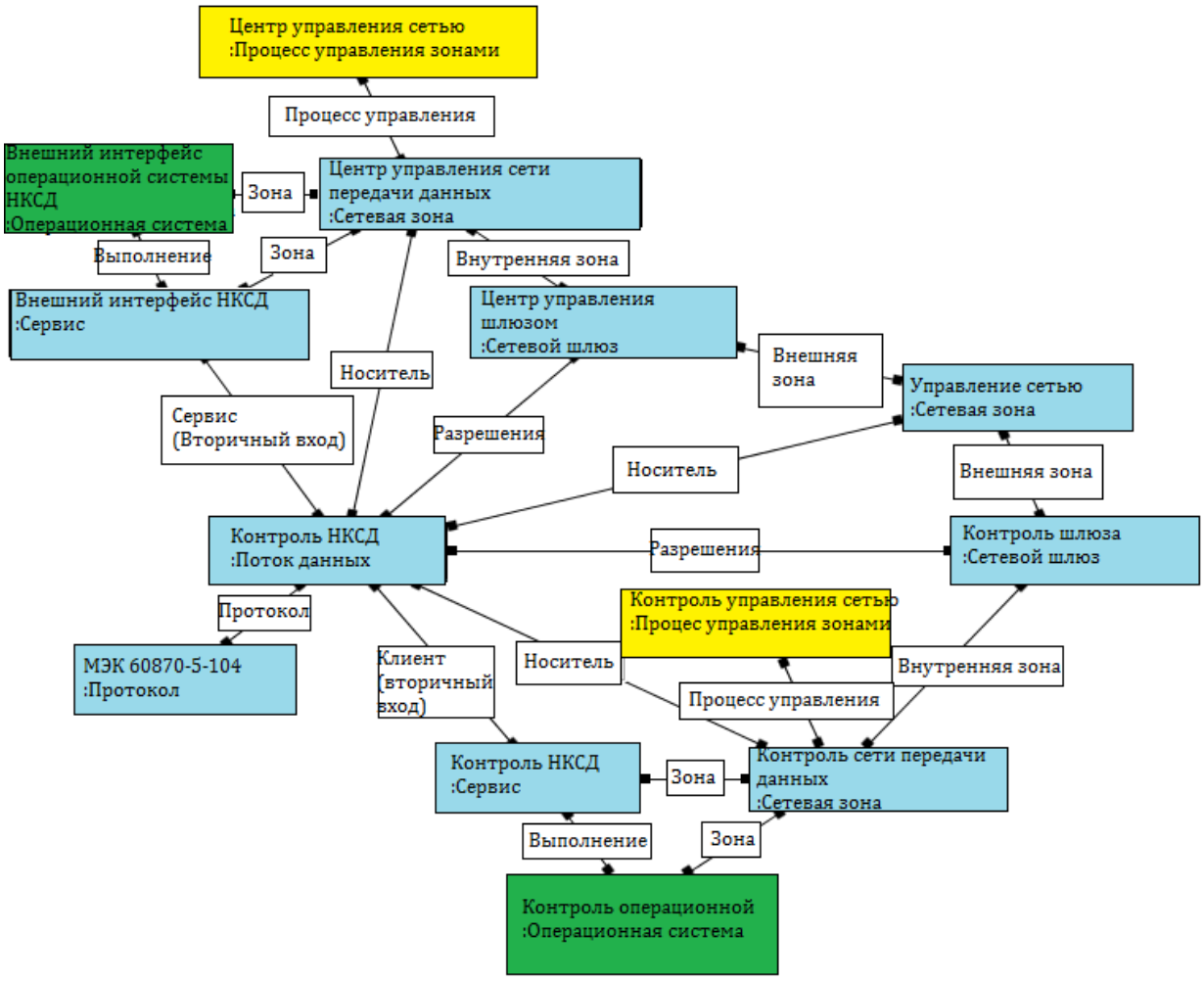

Рисунок 5-10 Поток данных наблюдения между системой НКСД в центре управления и подстанцией НКСД (вместе с несколькими близлежащими предприятиями) смоделированных на языке CySeMoL

Объект	Предположения
Рабочие станции и серверные операционные системы	Во многих системах (но не во всех) функционируют брандмауэр. В частности, невозможно было оборудовать подстанции и устройства РЭР хорошо настроенным брандмауэром.

Операционные системы автоматизированной рабочей станции	В центре домена в основном расположены современные рабочие станции, которые используют недавно выпущенные операционные системы (т.е., Windows 7 по сравнению с Windows XP или более старой версией). Хотя системы автоматизированной рабочей подстанции являются специализированными (в противоположность общедоступному), двоичные файлы могут быть получены с помощью антагонистов, так как системы известны и широко используются (например, Windows). Не было возможности обновить подстанции и компоненты РЭР.
Серверная операционная система	Системы, как правило, легко поддаются ремонту и используют последние операционные разработки (обычно на базе Linux, поэтому с открытым доступом). Системы, восприимчивые к контролю электрического процесса (включая процессы в подстанциях), являются исключением, начиная с постоянного периодического обновления систем, восприимчивых к процессам управления, устанавливающих высокие требования к проверке и постоянству / совместимости рисков, на основе которых редко производятся обновления.
Выключатели и шлюзы (сетевая инфраструктура)	В центрах управления шлюзы используют статические APR-таблицы, и выключатели используют порт безопасности, который запрещает подключение неизвестных интерфейсных блоков.
Удаленный доступ клиентских приложений	Как правило, установлены клиентские приложения новых версий (применение вставок в программу последних версий).
Уровневые системы предприятия (например, система управления активами) и системы НКСД	Данные системы являются собственностью компании, и таким образом исходный код недоступен «взломщику».

Инфраструктурные системы (например, сервер ПСВ, услуги удаленного доступа)	Данные системы являются общедоступными, а также используются на основании протокола с общим доступом (напр., сетевой протокол прикладного уровня).
Сервисы и приложения	Приложения и сервисы, такие как удаленный доступ, по аналогии с операционными системами, подверглись значительному исследованию их кибербезопасности, а также увеличению срока их службы. В данном случае не рассматриваются процессы управления сервисами и приложениями, которые в большей степени проверены относительно базовой функциональной корректности и устойчивости процесса. Скорее речь идет о кибербезопасности.
Сетевое управление	Сетевое управление обычно работает согласно передовым методам операторов системы распределения в центре управления ИКТ. В центре управления ИКТ оператора системы распределения, не все системы регулярно обновляются, так же стоит принять во внимание нечастые аудиты в области безопасности. Кроме того, на уровне подстанции не проводятся регулярные регистрационные обзоры.
Программа осведомленности в области безопасности	Программа осведомленности в области безопасности предназначена для персонала ИКТ-обслуживания и операторов контроля. Для технического персонала, работающего на уровне подстанции, данная программа недоступна.

Протоколы связи	Протоколы удаленного доступа и протоколы, основанные на SSH, TLS или SSL, такие как HTTPS зашифрованы криптографически и прошли проверку подлинности. Процесс управления протоколов не является ни зашифрованным, ни криптографически подлинным. Сетевой протокол синхронизации времени не использует шифровальных методов. Доменные сервисы (X.500) и центр обновления Windows (MS-WUSP) используют шифровальную идентификацию, но не обфускацию (коммуникационное шифрование). Протоколы связи управления процессов не являются ни зашифрованными, ни криптографически подлинными.

Таблица 5-1: Краткое описание предположений для модели на языке CySeMoL

Таким образом, мы представляем оценку трех вариантов ИКТ-архитектуры, показанной выше. Три варианта ИКТ-архитектуры представлены в таблице 5-2.

Вариант	Специфика настройки
Вариант 1	Безопасность IP, основанная на ВЧС защите производится с помощью шлюзами, и обеспечивает связь, проходящую только через промежуточные сети.
Вариант 2	Подобно варианту 1. Исключением является то, что ВЧС предусматривает сеть контроля оператора системы распределения и управленческую сеть ИКТ ОСР, но не DER контроля сети распределительных энергоресурсов.
Вариант 3	Основан на безопасности транспортного уровня ВЧС и поддерживает схему "узел-узел", с помощью которой защищает связь, проходящую через промежуточные сети, а также через локальные сети.

Таблица 5-2: Описание оценки трех вариантов ИКТ-архитектур

5.4.4 Оценка безопасности при использовании языка CySeMoL

Для каждого варианта ИКТ-архитектуры мы проанализировали семь целей атаки. Цели были выбраны согласно их предполагаемой чувствительности, к потенциалу кибер-

диверсии электрического процесса в умной сети. Цели атаки перечислены в таблице 5-3. Есть два типа источников атаки. Во-первых, мы смоделировали внешние атаки. «Внешний взломщик» был смоделирован в качестве какого-либо объекта, снабженного компьютером и способного к доступу при использовании вредоносного пути к промежуточной сети (т.е., сетевое управление ОСР, управленческая сеть ИКТ ОСР и сетевое управление РЭР). Во-вторых, мы смоделировали внутренние атаки. "Внутренний взломщик" был смоделирован как объект, способный выступать в роли ИКТ-администратора, у которого была возможность применять удаленный доступ и соответствующую операционную систему автоматизированной рабочей станции в сети обслуживания ИКТ ОСР. Для каждой пары источника и цели атаки существует большое количество потенциальных путей. Для каждого сценария мы только рассматриваем наиболее вероятные виды атаки (самые простые примеры атаки, описанные на языке CySeMoL). На Рис. 5-11 представлен подобный сценарий нападения. В этом конкретном примере отправная точка нападения, как предполагается, является сетевое управление ОСР (выделенная желтым прямоугольником), где хакер получил доступ. Целью является внешний интерфейс НКСД центра управления ОСР (красный прямоугольник). Согласно вычислениям, самый вероятный путь состоит в следующем: сначала ОСР диспетчерского центра рассматривает плохо настроенный брандмауэр (который предполагает, что у нас нет полного понимания его реального положения) (шаг 8 – есть 35%-й шанс, что атака произошла). После этого предполагается возможность подключения к интерфейсной части НКСД без каких-либо проблем (шаги 9 и 10 – до сих пор существует 35%-ая вероятность осуществления атаки). Затем можно сказать, что есть некоторая вероятность того, что внутри интерфейсной части существует высокий уровень серьезной уязвимости (согласно CVSS[9] [5-31]) в обслуживании внешнего интерфейса, к которому также существует легкодоступный эксплойт (вредоносный код), которым использует хакер (шаги 11 - 14 – есть 32%-й шанс, что «взломщик» может использовать данный способ). (Данная информация является предупреждением о том, что у нас нет точных знаний о подобном виде уязвимости, а также данные об эксплойтах известны только для интерфейсной части.)

Наконец, хакер запускает произвольный код выполнения атаки, и совершая это действие, достигает полного контроля над операционной системой внешнего интерфейса (шаги 15 - 17 – финальная вероятность достижения данного состояния составляет 5%. Предполагается, что, если произвольное кодовое нападение произведено успешно, что

[9] http://www.first.org/cvss-guide.pdf

само по себе имеет довольно низкую вероятность, то производится полный доступ к операционной системе).

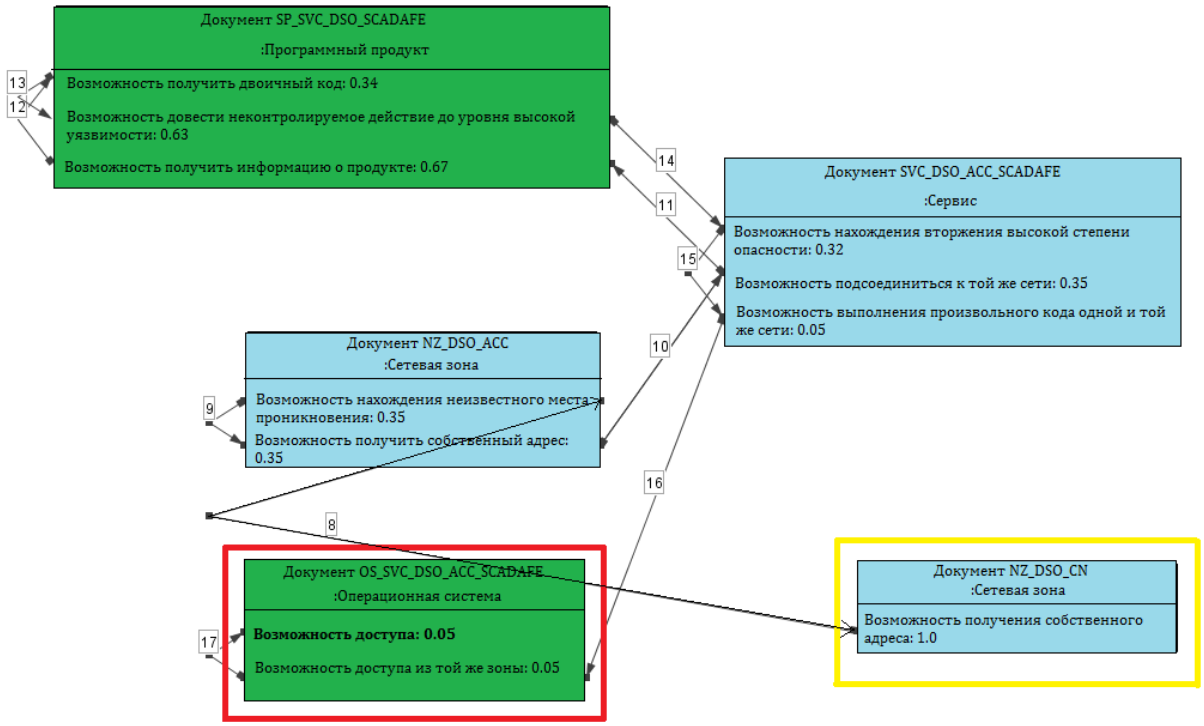

Рисунок 5-11 Пример пути атаки представленный на языке CySeMoL. Шаги нападения отмечены согласно числам на стрелках, и совокупная вероятность следования за нападением демонстрируется после шага нападения (шаги нападения 1-7 были пропущены для удобства)

В таблице 6-3 показаны итоговые результаты (вероятности атаки) для всех сценариев – для внешних и внутренних атак (в круглых скобках). Для ясности они также предоставлены на рисунке 5 - 12. Результаты будут продемонстрированы ниже.

Цель атаки	**Вероятность условного успеха нападения для постороннего (посвященное лицо) в:**		
	Вариант 1	**Вариант 2**	**Вариант 3**
Система НКСД HMI центра управления ОСР	.15 (.4)	.41 (.4)	.08 (.4)
Внешний интерфейс НКСД центра управления ОСР	.05 (.4)	.47 (.4)	.09 (.4)
Уровень подстанции НКСД	.11 (.38)	.13 (.38)	.11 (.38)
Подстанция шлюза	.17 (.19)	.21 (.19)	.21 (.19)
Управление передачи между центром управления и подстанциями	.33 (.38)	.99 (.38)	.17 (.05)

Управление передачи в пределах подстанций	.32 (.37)	.98 (.37)	0.0 (.05)
Управление передачи между подстанциями и РЭР	.32 (.37)	1.0 (.37)	0.0 (.05)

Таблица 5-3: Результаты оценки проектирования на языке CySeMoL

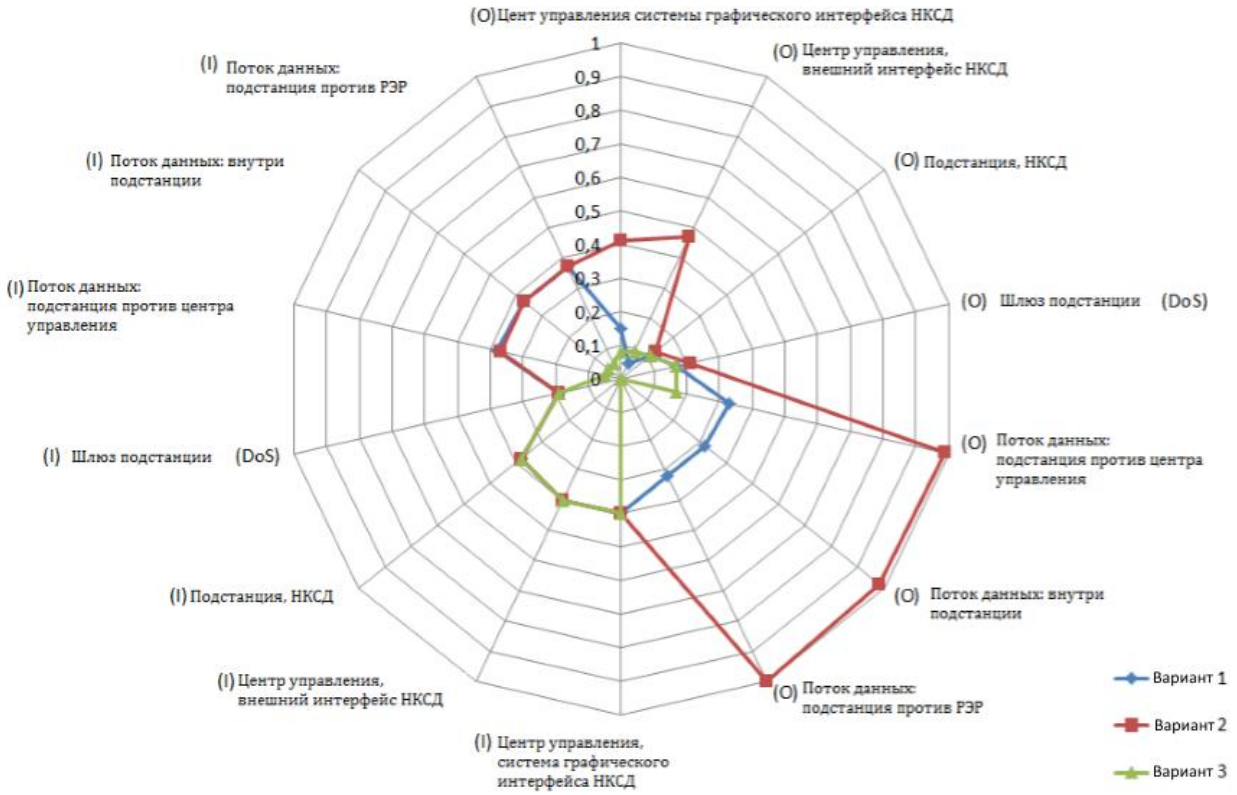

Рисунок 5-12 Подготовленное заключение результатов оценки на языке CySeMoL

Исходя из результатов видно, что вариант 2, который не использует защиту виртуальной частной сети (ВЧС) для передачи через сеть управления ДЭР (т.е. между подстанциями и ДЭР), кажется, безусловно, менее безопасными. Поскольку внешние атаки первоначально увеличиваются посредством потоков данных процесса управления, процесс связи кажется высоко уязвимым, говоря о том, что они находятся под угрозой (если атака произошла). Следовательно, внешний интерфейс НКСД и система НКСД HMI центра управления ОСР становятся особенно легкими целями. Уровень подстанции НКСД также кажется более уязвимым. Следующий худший вариант-это вариант 1, который, с другой стороны, кажется значительно безопаснее, чем вариант 2 – благодаря незначительному недостатку, например, отсутствие защиты связи в ненадежной сети. Осуществление защиты ВЧС межхостовым способом (так же, как и в

модуле TLS ВЧС), которая обычно обеспечивает защиту связи вне источника, места расположения хоста и накопителя ВЧС (шлюзы), приводит к неспособности хакера поставить под угрозу потоки данных, направленные от одного компьютера к другому. В целом, оценки показывают, что защита ВЧС - важная контрмера в данном типе архитектуры, и что защита модуля TLS ВЧС превосходит защиту IP безопасности ВЧС, так как это защищает большую часть связей.

5.5 Заключение

Целью рабочего направления была демонстрация того, что построение графа атак является одновременно существенным и целесообразным методом для анализа кибербезопасности системы управления архитектурами будущих умных сетей. Моделирование атак подразумевает несколько типов «нападений». В данной работе был представлен один из самых простых подходов (деревья атаки), который был использован в примере. Работа указала на ценность этого простого в использовании подхода как средства для получения первого целостного понимания достоинств и недостатков системного архитектурного решения. Модель, подобная этой, может быть при необходимости может быть рассмотрена подробно.

Анализ кибербезопасности ИКТ-архитектуры становится более значимым в будущих приложениях умной сети, характеризуемых многократными и разнородными коммуникационными связями для критических сетевых систем управления. Применение инструментов моделирования и оценки, обеспечивающих анализ безопасности, позволяет регулировать сложность корреляции составляющих конфигураций с этапами атак и мерами обеспечения безопасности. Основываясь на предположении, что конфигурации архитектуры являются фундаментальным элементом кибербезопасности умной сети, в данной работе было исследовано применение структуры графа атаки, язык CySeMoL, к анализу безопасности архитектурных вариантов для регулированного напряжения в активных распределительных сетях, соединяющих распределенные энергоресурсы.

Мы представили архитектуру управления напряжением, используя язык CySeMoL, и оценили вероятность атаки, сравнивая три варианта конфигурации, где атака произведена успешно. Оценка на языке CySeMoL показала несколько различий среди вариантов конфигураций исследованной ИКТ-архитектуры. Исходя из предварительных оценок, можно прийти к заключению, что надежность

сложившейся вероятности значений увеличивается в соответствии с архитектурой и моделями атаки, захваченными программой базы данных, в момент неточного уменьшения конфигураций архитектуры, представленных количеством предположений, используемых в оценке. Однако, имея под рукой реальную и более подробную архитектуру, возможно, из анализа были бы получены более точные результаты. Кроме того, CySeMoL - упрощенная, однако, всесторонняя метамодель, которая объединяет много различных разделов в пределах области кибербезопасности. Как таковой, это может быть мощный инструмент для ИКТ-архитекторы, который рассматривает различные альтернативные варианты или способствует их развитию с целью обеспечения умной сети для тех, кто мог бы принять во внимание руководство по объекту в установленных моделях кибербезопасности, проводить эксперименты и использовать знания, полученные от экспертов в области кибербезопасности.

Применение текущей версии языка CySeMoL к вариантам архитектуры Регулирования Напряжения также позволило определить характерные аспекты, которые до этого не рассматривались, например, данные протоколов связи и мер безопасности. Дальнейшее применение языка CySeMoL к архитектуре умной сети обеспечит результаты о соответствии данной структуры к сектору умной сети.

Работа также привлекла внимание ко многим проблемам, которые все еще встречаются при применении графической атаки, моделирующей программно-аппаратную энергосберегающую технологию. Очевидно, использование графической атаки, смоделированной в качестве практического применения, требует многих компромиссов, начинающихся с выбора любого метода моделирования (такого как деревья атаки) или использования более сложных вероятностных и динамических доступных подходов. Кроме того, уровень данных, используемых для описаний действий умной сети, оказывает некоторое влияние. Для полной модели больше данных должно быть добавлено в отношении к различным (ИКТ) компонентам системы и к описанию других умных сетей управления функциями. Аналогично, другие процессы атаки и дополнительные цели, которые не были представлены в примере, так же должны быть рассмотрены. Добавленные к этому контрмеры, возможно, также должны быть включены. И наконец, чтобы графическое моделирование атаки стало целесообразной поддержкой для ЭЭК при принятии решений, последствия различных атак, как на энергосистеме, так и во время рабочего

процесса в целом, должны быть подробно рассмотрены. Многие из этих аспектов остаются на этапе дальнейшей разработки.

6 Третье рабочее направление: дистанционное обслуживание

Целью данного рабочего направления является изучение следующих аспектов:

• риски обслуживания сторонней организации и информация, передаваемая к/от партнерам(ов);

• правила и методы наиболее успешной практики для технического обслуживания сторонних организаций, а также информация, направленная к/от иностранным партнерам(ов).

Ниже представлены лица, сделавшие вклад в разработки третьего рабочего направления:

- Паскаль Ситбон, "Electricite de France", Франция
- Кристоф Пойриер, «Electricite de France ", Франция
- Йенс-Тобиас Цербшт, «Vattenfall», Швеция
- Марк Шерер, «Alstom Grid», Франция
- Роберт Иванс, «Snowy Hydro», Австралия
- Марк Тричлер, консалтинговая фирма «PA», Великобритания
- Д. К. Хольстайн, консалтинговая группа «OPUS», США

6.1 Область применения и цели

Электроэнергетические компании зависят от удаленного доступа для некоторых вариантов использования, таких как обслуживание или контроль. При одновременном повышении производительности и улучшении процесса в целом, данные соединения протекают с некоторым риском. В этой главе мы сосредотачиваемся на вопросах удаленного доступа сторонних организаций. Здесь мы рассматриваем использование ресурсов информационно-коммуникационных технологий (ИКТ) (компьютер, сеть и др.), которые не контролируются электроэнергетическими компаниями при доступе к внутренним ресурсам, находясь вне физической границы электроэнергетической компании в момент оказания услуги.

В данной главе предложено руководство для электроэнергетических компаний для того,

чтобы выбрать соответствующие стандарты или методы передовых технологий, кроме того, представлен контрольный список для проведения процесса и рассмотрение универсальной архитектуры. Дальнейшее изучение могло бы способствовать созданию расширенного технического руководства и более подробного анализа дистанционного управления потенциально опасными объектами.

6.2 Источники угроз

Автоматизированные Системы Управления (АСУ) более уязвимы через их удаленный доступ обслуживания. Сеть Shodan пролила свет на недостатки ИКТ, как описано в статье газеты Washington Post за 2012 год [6-1]. Угрозы зависят от типа удаленного доступа и от внедренной архитектуры. Ниже представлены некоторые недостатки и уязвимости, часто связанные с удаленным обслуживанием ([6-2] здесь приводится более подробный анализ угроз ИКТ-инфраструктур):

- Постоянная связь с Интернетом и / или связь безопасных систем с системами более низкого трастового уровня (эти системы, вероятно, появятся в сетях Shodan и Google из-за специалистов, случайно выкладывающих конфиденциальную информацию в интернет)

- Ненадежные (всемирно известные) пароли или их отсутствие

- Слабые места в интерфейсах логина (обычно известны благодаря широкому применению оборудования, изготовленного с максимальным использованием коммерчески доступных элементов)

- Редко обновляемая базовая операционная система

- Нет регистрации рабочих действий

- Люди, отвечающие за отдаленные системы обслуживания, которые не обучены для данной должности, или, которые не могут выявить проблемы в безопасности

- Отсутствие обнаружения атаки / автоматическое предупреждение при происшествиях, относящихся к безопасности.

Наличие недостатков на отдаленной системе обслуживания может привести к атакам ИКТ и оказать влияние на все операции ЭЭК.

Главные риски, связанные с отдаленными системами обслуживания:

• Необнаруженное вторжение незарегистрированного пользователя в систему (использование ненадежного пароля, пути обхода системы защиты или уязвимости программного обеспечения) при оказании воздействия, зависящего от цели «взломщика» и его навыков (это - самая большая угроза согласно руководству Британского института стандартов (BSI) [6-3])

• Нарушение доступа к системе, которая может привести к глобальному повреждению целой информационной системы

• Нарушение в конфиденциальности или целостности данных информационной системы

• Несанкционированная модернизация прав для отдаленного технического специалиста во время операции по обновлению

Данный тип нарушения уже встречался ранее: одна из первых публично известных успешно проведенных атак произошла в 2000 году. Австралиец, под влиянием эмоций в связи с отклонением запроса на принятие на работу в компанию «Maroochydore Shire Council», дистанционно открыл клапаны сточных вод, которые привели к загрязнению и уничтожению морской флоры и фауны. Одно из последних широко известных нарушений совершил 22-летний американец 17-го ноября 2012 года, который вывел из строя насос, взломав Спрингфилдскую систему очистки воды, которая использовалась шестнадцатью тысячами жителей Техаса. Число этих атак растет каждый день, что подняло вопрос об ИКТ-взломах на повестку дня для многих организаций, как сообщают доклады Trend Micro [6-4], [6-5].

Чтобы противостоять растущему числу угроз, было разработано два типа мер обеспечения безопасности: первый – это контрольный список вопросов при заключении контракта со сторонними организациями, а второй – пропагандированное технических средств управления, предоставляемых современными архитектурами удаленного доступа.

6.3 Проблемы при заключении контрактов: требования безопасности для электроэнергетических компаний.

На практике часто сложно осуществить методы коллективной безопасности в системах управления промышленными процессами электроэнергетических компаний ввиду ограниченности имеющихся ресурсов и, в том числе, времени. Другой важный вопрос – проблемы при заключении контрактов. Предоставление удаленного доступа сторонними

организациями само по себе не может быть простым процессом, так как у электроэнергетических компаний и сторонних организаций различные обязательства, подходы к управлению рисками, а иногда и политика безопасности. Например, владелец / оператор не всегда имеет возможность выбрать, что может осуществиться без согласования с поставщиком услуг. Требования, предъявляемые к кибербезопасности, должны относиться ко всему жизненному циклу продукта, начиная с его дизайна, затем к тестированию, обслуживанию и поддержке, списанию и уничтожению.

Рисунок 6-1 Этапы жизненного цикла информационной системы согласно Департамент Юстиции США (перерисовка Юджином Винсентом Тэнтогом для Википедии)

Существует множество стандартов, директив и передовых методов в сфере кибербезопасности. В большей степени они относятся к требованиям по кибербезопасности к оператору электроэнергетической системы для создания надежной программы для защиты информации, эффективного управления программой и установки контроля за безопасностью, чтобы минимизировать известные угрозы основным ресурсам. В основном эти требования относятся к контролю доступа (идентификация, аутентификация и авторизация), конфиденциальности и подлинности данных, ограничению сетевых доменов и потоков данных, системам обнаружения, управлению инцидентами и проверке доступности ключевых ресурсов. Все больше принимаются во внимание такие специфические особенности промышленных систем, как техника безопасности, главенство доступности и целостности над конфиденциальностью, архитектурные и системные ограничения и т.д. Примерами являются языки для

управления системами, обеспечивающие кибербезопасность, разработанные Министерством внутренней безопасности (МВБ) и Министерством энергетики США [6-6,6-7], Электроэнергетическим научно-исследовательским институтом [6-8,6-9], стандарты WIB M2784X10 [6-10] или ИСО / МЭК 27036 [6-11], Национального института стандартов и технологий США 7628 [6-12], ИСО / МЭК 62443 [6-13], ИСО / МЭК 27019 [6-14] и защита объектов жизнеобеспечения Североамериканской корпорации по обеспечению надежности электросистем [6-15]. Некоторые из них отмечены на рис. 7-2.

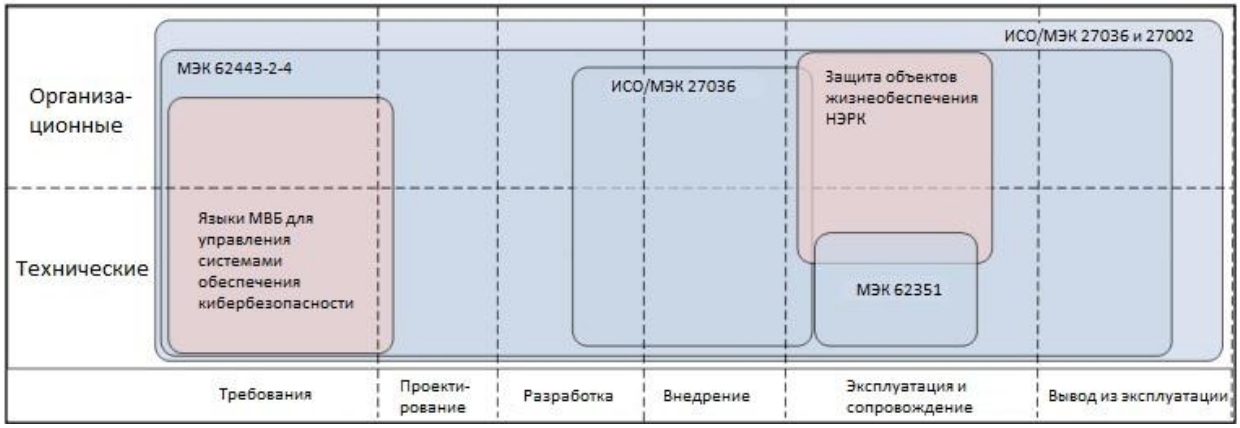

Рисунок 6-2 Существующие стандарты и передовые методы

Некоторые стандарты (например, МЭК 62351) включают требования к функциональной совместимости безопасности для выбранных протоколов передачи данных. Другие стандарты относятся к традиционным системам, использующим последовательные протоколы передачи данных (стандарты Института инженеров по электротехнике и электронике P1689 [6-16]). Все ресурсы представляют собой превосходный источник для обеспечения различных нужд электроэнергетических компаний, например:

- Технический контроль, например, стандарты ИСО/МЭК 27002
- Материально-техническое снабжение, такое как язык для управления системами, обеспечивающий кибербезопасность, разработанный Министерством внутренней безопасности США, включающийся в запрос котировок [6-6]
- Анализ рисков или системы управления в организациях, например, стандарты ИСО/МЭК 27001
- Особый контроль, относящийся к электроэнергетическим компаниям, например, стандарты ИСО/МЭК 27019 или МЭК 62443

Чтобы улучшить материально-техническое снабжение требований безопасности, была определена схема градации, которая должна упростить процесс сравнения и оценки

степени безопасности в предложенном решении. Также рассматриваются различные типы контрактов и сопутствующие стимулы для поддержки безопасности [6-17]. Данный подход был успешно протестирован на шлюзопередающей электроэнергию подстанции, и в будущем его можно адаптировать для удаленного доступа, предоставляемого сторонней организацией.

В таблице 6-1 мы предлагаем контрольный список вопросов для электроэнергетических компаний, чтобы помочь быстро определить необходимые положения до установки удаленного доступа сторонней организацией. Этот контрольный список нельзя назвать исчерпывающим: его целью не является замена существующих стандартов и передовых методов, его предназначение - убедиться, что защита была действительно установлена.

Бизнес-потребности и нужды	
□	Опишите бизнес-потребности (напр. мониторинг, техобслуживание и т.д.) и объем работ
□	Опишите постоянные бизнес-потребности
□	Опишите потребности в области связи (напр., постоянные/по требованию, пропускная способность, время задержки)
□	Опишите ресурсы и их классификацию / потребность в защите
□	Рассмотрите альтернативные решения для осуществления удаленного доступа сторонним разработчиком (внутренним персоналом, через локальный доступ)
□	Проведите/обновите оценку рисков рассматриваемого объема работ
□	Включите все заинтересованные стороны электроэнергетической компании в одну систему (напр., руководителя по информационной безопасности, отдел разработки, специалистов по информационным технологиям, отдел закупок)
Организационные требования безопасности	
□	Определите организационные требования безопасности, например: • Совместимость/актуальность для существующей организационной политики электроэнергетической компании, • Управление инцидентами и отчетность, • Требования к сертификации подрядчика
□	Определите периодичность пересмотра требований к безопасности
□	Определите, как можно контролировать средства обеспечения безопасности фирмы-подрядчика (напр., внутренний/внешний контроль, регистрация данных)
□	Определите задачи и обязанности для каждого объекта
□	Запросите у фирмы-подрядчика описание средств обеспечения и стратегии безопасности (напр., система снабжения, управление инцидентами)
Требования к отделу кадров	
□	Определите требования безопасности (напр., требования к проверке данных, работе Управления по выводу из эксплуатации ядерных объектов Великобритании, уничтожению учетных записей)
□	Определите требования к удостоверяющим документам (напр., наличие сертификатов, образования, опыта работы)
□	Определите требуемые мероприятия (напр., обучение сотрудников, осведомление)
Технические требования безопасности	

□	Определите требования сетевой безопасности (напр., сетевые периметры, сетевые протоколы, управление сетевым доступом)
□	Определите систему управления и основные эксплуатационные характеристики, например: • Жесткую стратегию (напр., ограничительные службы, финансовая отчетность) • Управление доступом • Политику обновления и проведения ремонтных работ • Общение с прессой
□	В случае необходимости включите требования к физическим средствам осуществления безопасности (напр., защита входа в здание, контроль доступа посетителей)

Таблица 6-1: Краткий обзор контрольного списка действий для электроэнергетической компании перед открытием удаленного доступа сторонней организации.

В разделе 6.5 мы также предлагаем расширенный список требований безопасности с совместными средствами управления для рассмотрения электроэнергетической компанией до заключения контракта на удаленный доступ со сторонней организацией. Электроэнергетическая компания имеет возможность выбрать значимые требования/средства управления, подходящие в их конкретном случае, и включить их в свой запрос коммерческого предложения.

6.4 Практическое применение на существующих архитектурах

Зачастую производители подключаются к своим системам и управляют ими удаленно. Это дистанционное обслуживание увеличивает подверженность внешнему воздействию, поэтому производителю следует свести эту возможность к минимуму и сделать выбор в пользу локального обслуживания, хотя бы для запланированных и не экстренных мероприятий.

По нашему мнению, существует три типа систем, которые могут обслуживаться дистанционно: критические системы, малые системы и все остальные. Электроэнергетическая компания вправе сама решать, необходим ли ей уделенный доступ к критическим системам при существующей системе безопасности, даже если данных подход не экономичен и не практичен. Решение должно быть принято руководством, однако существуют стандарты [6-14] и единые государственные рекомендации [6-18], [6-19], [6-20] препятствующие дистанционному обслуживанию систем безопасности в

компаниях, облагая технический контроль высоким налогом. Выбранная архитектура должна поддерживать решение руководства и обеспечивать защиту и безопасность.

Как отображено на рис.7-3, структура удаленного доступа имеет несколько компонентов:

- Субъекты сторонней организации (СО) - пользователи, которые получат доступ к ресурсам;
- Ресурсы информационно-коммуникационных технологий сторонней организации (ИКТ СО), которые используются для выполнения действий в режиме удаленного доступа;
- Сеть доступа, которая может быть сетью общего пользования;
- Сфера архитектуры доступа электроэнергетической компании, которая сама по себе состоит из ресурсов, которые находятся в открытом доступе, а также компоненты безопасности, предназначенные для изолирования и защиты разных сфер и обеспечения доступа к этим ресурсам;
- Зона внутренних ресурсов электроэнергетической компании, которая обычно остается недоступной для сторонней организации.

В зависимости от контракта, обязанности могут быть разными, как это показано стрелками. Конечно же, возможны и несколько реализаций, например, использование сети общего пользования типа сети Интернет или специальной сети, различных схем аутентификации, протоколов безопасности виртуальной частной сети, управление строго ограниченной зоной со стороны электроэнергетической компании для доступа к ресурсам сторонней организации и т.д.

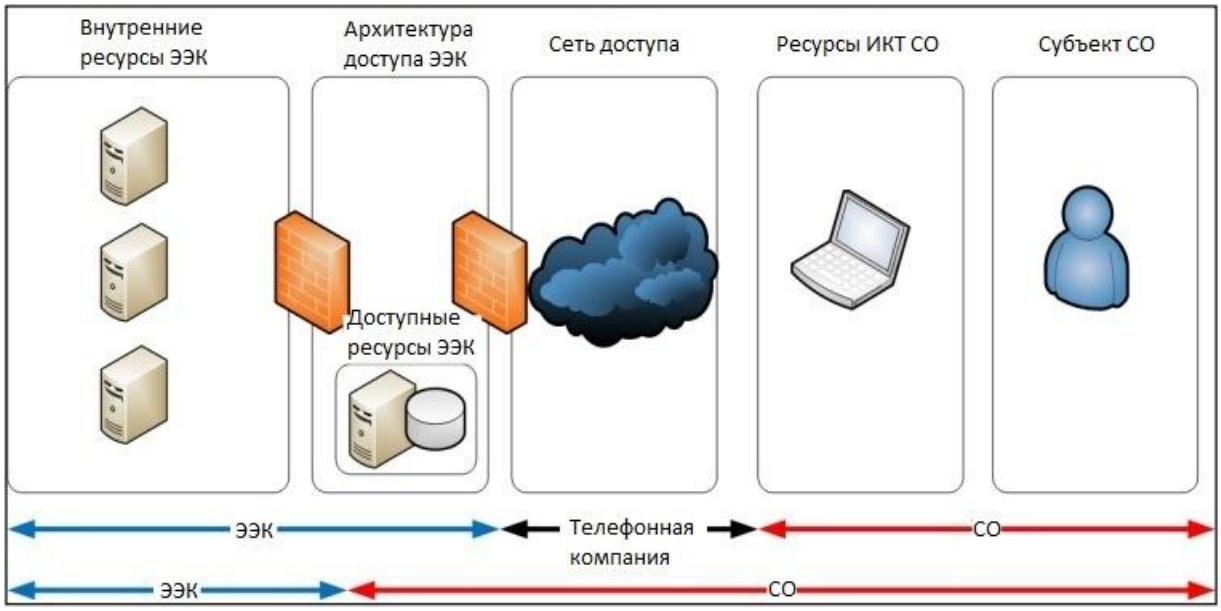

Рисунок 7-3 Обобщённая архитектура удаленного доступа

Выбор архитектуры зависит от ограничений, потребностей и системы управления риском электроэнергетической компании. Основным критерием является руководство информационным потоком. Одного только выходного потока от электроэнергетической компании к сторонней организации может быть достаточно для, например, сбора системных журналов для дальнейшего анализа (примеры включают регистрацию неисправностей из цифрового аварийного регистратора или защитных реле, информацию по управлению активами и т.д.). Удаленный доступ может быть ограничен созданием изолированной зоны, которая может принадлежать архитектуре доступа электроэнергетической компании, но не иметь доступа к ее зоне внутренних ресурсов.

Зеленая стрелка на рис. 7-4 (независимое извлечение файлов) представляет собой пример архитектуры с одним только выходным потоком. Чувствительные устройства отправляют свои данные платформе извлечения данных внутри децентрализованной зоны. Коммуникация этих платформ с чувствительными устройствами невозможна (даже подтверждение приема сообщения), благодаря брандмауэру между подстанцией и офисом. Брандмауэр может быть заменен диодом (на физическом уровне сетевой модели взаимодействия открытых систем) для более эффективной защиты.

Требуется дополнительная осторожность при извлечении корпоративного протокола организации-поставщика, когда необходима двунаправленная схема соединения (отмечена красной стрелкой на рис. 7-4).

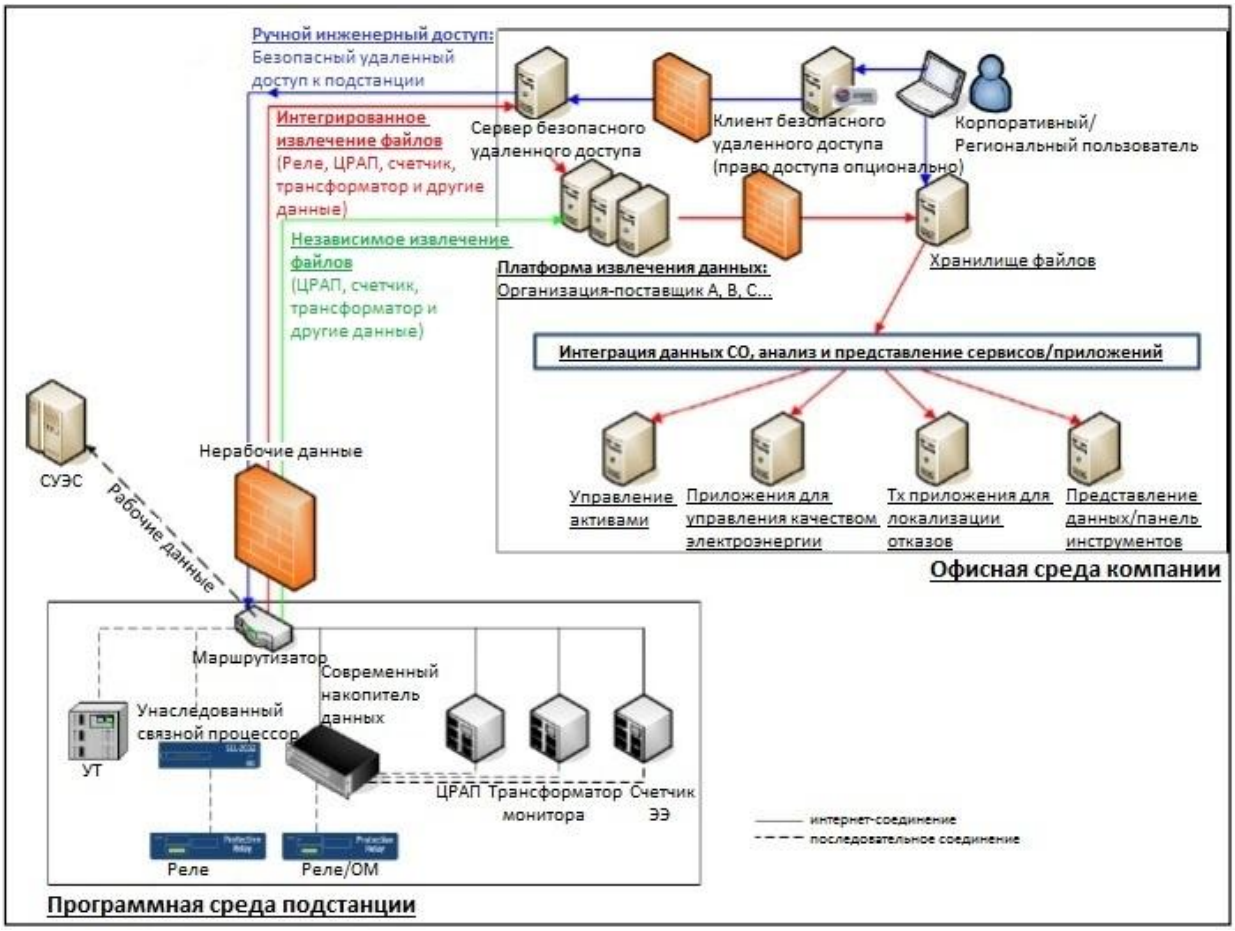

Рисунок 7-4 Архитектура удаленного доступа (источник: Электроэнергетический научно-исследовательский институт [17])

Вот некоторые передовые методы и эталонные архитектуры, описанные в общедоступных стандартах ([6-14], [6-15], [6-13], [6-19]), и руководства ([6-18], [6-20], [6-21], [6-22], [6-23], [6-24], [6-25], [6-26], [6-27]).

Основными целями архитектуры являются:

- Строгий контроль доступа на всех значимых уровнях, в том числе на сетевом, функциональном, информационном уровне
- Предотвращение использования уязвимых сторон или путей обхода защиты системы на устройствах удаленного обслуживания
- Сохранение конфиденциальности и целостности данных
- Обеспечение регистрации всех удаленно выполняемых действий техническими специалистами сторонней организации
- Обеспечение безопасности удаленного обслуживания для остальной части системы (в частности, с точки зрения доступности)
- Предотвращение утечки данных

Не должны допускаться прямые коммутируемые подключения к системам или применяться те же средства управления безопасностью, что и для шлюза безопасности. Если необходимо удаленное обслуживание, то должны использоваться следующие средства управления безопасностью:

- Ведение журнала регистрации для доступа и подключения и использование только именных учетных записей для отслеживания действий отдельных лиц. Требуется установка таймера неактивности и максимального времени соединения, чтобы убедиться в отсутствии совместного использования сеанса.
- Ведение журналов регистрации операций.
- Использование шифрования для внешнего потока данных.
- Использование двухфакторной аутентификации.
- Удаленный доступ должен исходить от специально выделенного компьютера в выделенной демилитаризованной зоне, и все управляемые системы должны только предоставлять разрешение на конфигурацию с этого выделенного компьютера.
- Компания должна обеспечить сегментацию ее внутренней сети, так, чтобы фирма-подрядчик имела доступ только к тем системам, к которым она должна быть подключена. Это должно осуществляться устройствами, управляемыми компанией, в частности, когда архитектура доступа контролируется сторонней организацией.
- Удаленное управление, осуществляемое сторонней организацией, должно использоваться только когда местный квалифицированный персонал готов к работе и следит за процессом (принцип четырех глаз, использующийся для возможности предотвращения нежелательных действий). Любое действия должно быть записано для дальнейшего анализа или экспертизы.

Прямое подключение системы к сети Интернет не рекомендуется, но может быть использовано, если предприятие не имеет общекорпоративного доступа к сети Интернет и/или для малых систем, установленных удаленно, наподобие тех, что используются при работе с распределенными энергоресурсами (небольшие фермы солнечных батарей, изолированные ветровые установки т.д.)

Цели компонентов	Внутренние ресурсы электро-энергетической компании	Архитектура доступа электро-энергетической компании	Сеть доступа	Ресурсы ИКТ СО	Субъект СО
Строгий контроль доступа на всех значимых уровнях, в том числе на сетевом, функциональном, информационном уровнях	- Предпочтение отдается только выходным потокам	- Установка отдельной децентрализованной зоны для простоты контроля - Сегментация фирмой-подрядчиком	- Отсутствие прямого подключения к сети Интернет	/	- Именной доступ - Уничтожение учетных записей - Двухфакторная аутентификация
Предотвращение использования уязвимых сторон или путей обхода защиты системы на устройствах удаленного обслуживания	- Предпочтение отдается только выходным потокам - Удаленное управление отдельной станцией - Принцип четырех глаз	- Защита управляющей станции	- Отсутствие прямого подключения к сети Интернет	- Использование выделенных устройств	- Отбор сотрудников - Образование
Сохранение конфиденциальности и целостности данных	/	- Сегментация фирмой-подрядчиком	- Использование шифрования - Сегментация сети фирмой-подрядчиком - Предпочтение частным сетям	- Использование выделенных устройств	- Отбор сотрудников - Процедура обработки

Обеспечение регистрации всех удаленно выполненных действий техническими специалистам и сторонней организации	- Удаленное управление отдельной станцией	- Установка отдельной демилитари-зованной зоны для простоты контроля	/	/	- Именной доступ
Обеспечение безопасности удаленного обслуживания для остальной части системы (в частности, с точки зрения доступности)	- Удаленное управление отдельной станцией - Принцип четырех глаз	/	- Физическое разделение сети подстанции и сети удаленного доступа	- Тестиро-вание на экспери-ментальных платформах до широкого использо-вания - Предпо-чтение автоматичес ких скриптов	- Отбор сотрудников - Уничто-жение учетных записей
Предотвра-щение утечки данных	- Удаленное управление отдельной станцией	- Защита управляющей станции	- Использо-вание шифрования	- Использо-вание выделенных устройств	- Процедура обработки - Образование - Отбор сотрудников

Таблица 6-2: Цели безопасности по каждому компоненту архитектуры удаленного доступа

В дополнение к ранее описанным передовым методам, таблица 6-2 показывает, как основные цели архитектуры безопасности поддерживаются техническими средствами управления, дополняющими друг друга. Она иллюстрирует передовой опыт по каждому компоненту архитектуры удаленного доступа.

6.5 Контрольный список требований безопасности и средств административного контроля для рассмотрения соглашений со сторонней организацией

Требования безопасности	**Средства административного контроля**
Политика безопасности в области информационных технологий сторонней организации	Применяется для удаленного доступа электроэнергетической компании Задокументированное освобождение от

	выполнения требований электроэнергетической компании Система соответствий требованиям
Роли и обязанности в обеспечении безопасности	Сотрудники, задачи, обязанности, определенные для осуществления удаленного доступа
Конфиденциальность для всех сотрудников сторонней организации, имеющих удаленный доступ	Соглашения о конфиденциальности – неразглашение информации электроэнергетической компании, средств управления безопасностью и уязвимых сторон
Обязанность предоставления информации	Сторонние организации должны информировать электроэнергетическую компанию о проблемах, уязвимых сторонах и аварийных ситуациях в сфере безопасности
Разделение сети и электронная охрана периметра	Создание обслуживаемой сетью документа, описывающего физическое и логическое разделение Управление конфигурацией и ресурсами Идентификация электронной охраны периметра Идентификация и средства управления точками доступа
Повышение уровня безопасности	Отключение неиспользуемых портов Удаление/отключение неиспользуемых служб

	Минимальная конфигурация
Связь по защищенным сетям	Шифрование сетевого трафика между сторонними организациями и электроэнергетической компанией Отключение незащищенного доступа, например, телефонной сети
Безопасность систем	Сохранение обновленного аудио/видео и предотвращение заражения вредоносным ПО Управление обновлениями ОС и приложений Управление конфигурацией Ограниченное использование удаленного доступа для поддержки систем Проверка нового оборудования в целях обеспечения безопасности
Необходимость в дополнительных средствах управления для мобильных систем (напр., ноутбуках)	Шифрование жестких дисков Локальный брандмауэр Политика ограниченного использования
Текущая оценка уязвимости	Порядок проведения, протоколирования, исправления оценок
Проверка безопасности персонала	Для ведения кадрового реестра и осуществления проверки безопасности сторонняя организация должна проверять сотрудников (Государственные законы о проверке)

Логическое управление доступом и управление учетными записями пользователей	Использование индивидуальных учетных записей и протоколов в кадровом реестре Надежные пароли/двухфакторная аутентификация Одобренные, зарегистрированные и проверенные привилегии пользователей Разделение обязанностей по управлению учетными записями пользователей Регистрация и анализ пользовательского доступа, в том числе неудачных попыток
Физические средства осуществления безопасности	Надежное расположение оборудования для осуществления удаленного доступа Разделение обязанностей для подтверждения доступа Регистрация и анализ физического доступа
Инструктаж	Регулярный инструктаж сотрудников сторонней организации по вопросам безопасности
Управление системами	Управление обновлениями и конфигурациями
Тестирование безопасности систем	Скрипты и протоколы тестирования безопасности
Обработка случаев нарушений безопасности	Регулярное тестирование поддерживаемой процедуры
Аварийное восстановление/устойчивость функционирования	Регулярное тестирование поддерживаемой процедуры

Таблица 6-3: Контрольный список требований безопасности и средств административного контроля для рассмотрения соглашений со сторонней организацией

6.6 Заключение

Электроэнергетические компании используют удаленный доступ для круга целей, например, для технического обслуживания или мониторинга. Но вместе с повышением производительности и скорости всего процесса появляются и новые риски. Чаще всего удаленный доступ осуществляется сторонними организациями, а несогласованность политик безопасности ведет к ослаблению предприятий.

В целях оказания поддержки усилиям компаний в этой области, мы предложили упрощенный контрольный список вопросов, который применим к удаленным службам. Ожидается, что этот контрольный список поможет понять, нуждается ли предприятие в удаленных службах, предоставляемых сторонними организациями, и какие требования должны быть включены в запрос коммерческого предложения.

Мы также обсудили возможные технические архитектуры и способы снижения рисков.

Дальнейшие шаги включают интеграцию обычных устройств для дистанционного обслуживания, обзор различных архитектур для дистанционного обслуживания, их техническое сравнение, проблемы и контроль за использованием мобильных электронных устройств (например, планшетов, смартфонов и т.д.) для осуществления дистанционного обслуживания, а также анализ вопросов, связанных с расширением удаленного доступа включая цели дистанционного управления.

7 Заключение и перспективы рабочей группы D2.31

Совмещение эксплуатационных и информационных технологий стало нормой. Коммуникационная инфраструктура и информационные потоки становятся все важнее для электроэнергетических компаний. В то же время промышленность становится все более популярной мишенью для хакеров и иностранных правительственных органов. Именно поэтому появилась необходимость рассмотреть вопрос об угрозах кибербезопасности и рисках для всех организаций, а также повысить осведомленность всех работников от операторов систем до руководства, включая поставщиков, партнеров и сторонних организаций.

Подкомитет D2 рабочей группы WGD2.01 провел глобальный опрос [7-1] в 2013 году с целью определить приоритеты проблем в рабочих и коммерческих информационных системах для электроэнергетических компаний. На основе этой информации создавались

новые рабочие группы и выяснялись предпочтительные темы для исследований в 2014 году и позднее. В данном опросе наиболее важной темой стала «Кибербезопасность для развивающегося бизнеса электроэнергетических компаний, методы организации и проведения работ и риски» из-за потребности в дистанционном управления и использовании мобильных устройств. Данная информация помогла выбрать стратегию формирования новых рабочих групп, которым было поручено изучение этой темы, когда рабочая группа D2.31 выполнила свои задачи. Таким образом, подкомитет D2 планирует поддерживать электроэнергетические компании последующими исследованиями в области кибербезопасности.

A.1 Акронимы и аббревиатуры

Акроним/аббревиатура	Расшифровка
AMI	Развитая инфраструктура измерений
ANSI	Американский национальный институт стандартов
CFR	Свода Федеральных постановлений США
CIAD	Управление и Диаграммы Информационной Структуры
CIP	Критическая защита инфраструктуры
CySeMoL	Язык моделирования кибербезопасности
EMS	Энергетические системы управления
IAEA	Международное агентство по атомной энергетике
ICS-CERT	Команда быстрого реагирования на кибератаки промышленных систем управления
ISA99/ ISA95	Комитеты Международного Общества Автоматизации
LAN	Локальная сеть
MMS	Архитектуры систем управления рынком
MMS	Служба мультимедийных сообщений
NEI	Институт ядерной энергетики (США)
NERC	Североамериканская корпорация по вопросам надежности электроснабжения

NERC	Североамериканская корпорация электрической надежности
NRC	Комиссии по ядерной регламентации США
PEP	Точка реализации политики
PERA	Модель, устанавливающая значение структуры предприятия
SeSa	Проект по обеспечению безопасности
SIS	Объединенная европейская информационная система
SSH	Протокол Secure SHell
TLS	Безопасность транспортного уровня
UML	Унифицированный Язык Моделирования
ВН	Высокое напряжение
ВЧС	Виртуальная частная сеть
ЕАСИБ	Европейское агентство по сетевой и информационной безопасности
ЕИСС	Европейский институт стандартов связи
ЕКС	Европейский комитет по стандартизации
ЕКЭС	Европейский комитет по электротехническим стандартам
ИКТ	Информационно-коммуникационные технологии
ИСО	Международная организация по

	стандартизации
ИЭУ	Интеллектуальное Электронное Устройство
КН	Контроль напряжения
МАГАТЭ	Международное агентство по атомной энергии
МВБ	Министерством внутренней безопасности
МЭК	Международная электротехническая комиссия
НИСТ	Американский Национальный институт стандартов и технологий
НКСД	Наблюдение, контроль, сбор данных
ОИЦ	Объединенный исследовательский центр
ОРГ	*Объединенная рабочая группа*
ОСП	Оператор Системы Передачи
ОСР	Оператор Системы Распределения
ПЛК	Программируемые логические контроллеры
ПОНЛ	Переключатели ответвлений на линиях
ПСВ	Протокол сетевого времени
РЭР	Распределенные энергоресурсы
СИБ	Стандарты сетевой информационной безопасности
СН	Среднее напряжение

СО	Субъекты сторонней организации
СУД	Система управления документами
УООСП	Универсальный Объектно-ориентированный Случай Подстанции
ЧМИ	Человеко-машинный интерфейс

A.2 Ссылки

[1-1] J.-T. Zerbst, S. Zimmermann, D.K. Holstein, and C. Poirier, "Towards an adapted classification methodology for graded security approaches in EPU architectures" CIGRE Symposium, Lisbon, 2013

[1-2] Source: Électricité de France (EDF), Smart grid Europe 2009 presentation at Smart Grids Europe conference, Barcelona, 2009

[1-3] Christiane Grefe, “Blackout”, Die Zeit 16/2014 http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk ettlingen

[1-4] Felix Lindner,”Licht aus!” c’t magazin 09/2014 http://heise.de/-2165153

[1-5] L. Pietre-Cambacedes , M. Tritschler and G. Ericsson, "Cyber security myths on power control systems: 21 misconceptions and false beliefs," IEEE Transactions on Power Delivery, Vol. 26, Issue 1, pp. 161-172, January 2011.

[1-6] R. Langer, “Robust Control System Networks - How to achieve reliable control after Stuxnet”, Momentum Press, New York, 2012

[1-7] ABB white paper: “Security in the Smart Grids”, 2009 http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09 %29_docnum.pdf

[1-8] Jacobs, Mike. "10 Years After Record Blackout, Is U.S. Any Better Prepared? (Op -Ed)."Live Science. TechMedia Network, 14 Aug. 2013. Web. 17 Apr. 2014. http://www.livescience.com/38905-is-nation-better-prepared-to-prevent-blackouts.html

[1-9] Kim Zetter, “Researchers Uncover Holes That Open Power Stations to Hacking”, wired.com, 2013 http://www.wired.com/2013/10/ics/

[1-10] G. Dondossola, F. Garrone, J. Szanto “Cyber Risks in Energy Grid ICT Infrastructures” in Critical Infrastructure Protection and Resilience in the ICT Sector, Paul Theron and S. Bologna Ed., IGI Global, 2013

[1-11] ICS-CERT Monitor “Incident Response Activity - October, November, December 2013”, 2013 http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf

[1-12] C. Wueest, Symantec, “Targeted Attacks Against the Energy Sector”, 2014

[1-13] Stefan Frei, “Vulnerability Threat Trends: A DECADE IN REVIEW, TRANSITION ON THE WAY”, NSS Labs, Inc., 2013

[1-14] J. Zerbst, M. Schaefer, I. Rinta-Jouppi, "Zone principles as Cyber Security architecture element for Smart Grids", Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES

[1-15] Nicolas Falliere, Liam O Murchu, Eric Chien, “W32.Stuxnet Dossier”, 2011http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[1-16] Symantec Security Response: Dragonfly: Western Energy Companies Under Sabotage Threat http://www.symantec.com/connect/blogs/dragonfly-western-

energy-companies-under-sabotage-threat-energetic-bear

[1-17] François Page, McAfee Labs,"Hacktivism Cyberspace has become the new medium for political voices", 2012

[1-18] Heather MacKenzie, „Shamoon Malware and SCADA Security", 2012 http://www.isssource.com/shamoon-malware-and-scada security/

[1-19] Marshall Abrams, Joe Weiss "Malicious Control System Cyber Security Attack Case Study Maroochy Water Services, Australia", 2008 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-
Study_report.pdf

[1-20] Ryan Naraine," Shodan search exposes insecure SCADA systems", 2010 http://www.zdnet.com/blog/security/shodan-search-exposes-insecure-scada-systems/7611

[1-21] Kevin Poulsen,"Slammer worm crashed Ohio nuke plant net", 2003 http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/

[1-22] European Commission, „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussel, 2013

[1-23] Cyberspace policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[1-24] L. Pièrre-Cambacédès, T. Kropp, J. Weiss, R. Pellizzoni "Cybersecurity standards for the electric power industry – a survival kit", Paper D2-217, CIGRE Paris Session 2008,
France

[1-25] The NIST Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security", September 2010. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[1-26] F. Cleveland, "List of Cybersecurity for Smart Grid Standards and Guidelines", May 2013.
http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf

[1-27] Smart Grid Coordination Group Set of Standards Working Group "First set of standards" version 2.0, November 2012.
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_first_set_of_standards.pdf

[1-28] see "Working-party on Instrument Behaviour" (WIB) web site at
www.wib.nl[1-29] NIST Cybersecurity Framework
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[1-30] Nuclear Energy Institute, NEI 08-09 Cyber Security Plan for Nuclear

Power Reactors (rev. 6), April 2010

[1-31] IAEA Nuclear Security Series No. 17, Reference Manual, Computer Security at Nuclear Facilities, 2011

[1-32] L. Pietre-Cambacedes, T. Quinn, L. Hardin "Cyber Security of Nuclear Instrumentation and Control Systems - Overview of the IEC Standardization Activities" IFAC conference on Manufacturing, Management and Control (MIM 2013), Invited session on Cybersecurity of Control and Safety systems, St. Petersburg, Russia, June 2013

[1-33] European-Commission, "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace," European Commission, Joint Communication JOIN (2013) 1 final, 7 February 2013

[1-34] European Network and Information Security Agency (ENISA), "Smart Grid Security,
Recommendations for Europe and Member States", 2012 -07-01

[1-35] SoES Project, "International Standards and Policies – Map and Analysis", Security of Energy Systems Project, Deliverable D2, 2014. http://www.soes-project.eu

[1-36] ECSWG, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," US Department of Energy, September2011

[1-37] Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on "Security for Information Systems and Intranets in Electric Power Systems", 2007

[1-38] Technical Brochure 419 of the WG D2.22 " Information Security for Electric Power Utilities (EPUs) — CIGRÉ Developments on Frameworks, Risk Assessment, and Technology", 2010

[2-1] J. Zerbst et al, "Graded approach to cyber-security for EPUs: Clarifying the security levels and zone concepts", Paper D2-02-B09, 2011 SC D2 Colloquium, Buenos Aires – Argentina.

[2-2] G. Dondossola et al, "Modelling of cyber-attacks for assessing smart grid security", Paper D2- 02-B10, 2011 SC D2 Colloquium, Buenos Aires – Argentina.

[2-3] J. Zerbst et al, "Cyber-attack modelling and security graded approach: key elements when designing security architecture for Electric Power Utilities (EPUs)", Paper D2-07, 2012 SC D2 Session, Paris - France.

[2-4] J. Zerbst et al, "Towards an adapted classification methodology for graded security approaches in EPU architectures", Paper D2-02-B09, 2013 Cigre Symposium, Lisbon – Portugal.

[2-5] M. Ekstedt et al, "Application of a cyber-security assessment framework to smart grid architectures" Paper D2-02-11, 2013 SC D2 Colloquium, Mysore - India.

[2-6] P.Sitbon et al, "Security in remote services used by EPUs", Paper D2-203-2014, 2014 SC D2 Session, Paris - France.

[2-7] J. Zerbst et al, "Status of Cybersecurity", Electra 276, October 2014.

[4-1] IEC 62443-1, 2008, "Industrial communication networks - Network and system security Part 1 Terminology, concepts and models", 7 et sqq.

[4-2] IEC 62254-1, 2003, “Enterprise-control system integration – Part 1: Models and terminology”, 185 et sqq.

[4-3] IEC 61226, 2005, “Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions”

[4-4] NIST 800-60 Volume II Revision 1, 2008, “SECURITY CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

[4-5] U.S. Nuclear Regulatory Commission (NRC), 2010, “Regulatory Guide 5.71 - Cyber Security programs for Nuclear Facilities”, pp. 35

[4-6] Idaho National Laboratory, 2006, “Control Systems Cyber Security: Defense in Depth Strategies”, online http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[4-7] American National Standards Institute (ANSI), International Electro technical Commission (IEC), International Society of Automation (ISA), ANSI/ISA - 99.00.01-2007, 2007, IEC 62443-1 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

[4-8] NSA, Defense in Depth. US National Security Agency

[4-9] International Standard Organisation (ISO), International Electrotechnical Commission (IEC), 1994, “ISO/IEC 7498-1 Information Technology – Basis Reference Model: The Basic Model

[4-10] Trusted Information Sharing Network for Critical Infrastructure Protection, 2008, “Defense in depth”, Available at: http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Publications_e-SecurityPublications (last visited 5th May2010)

[4-11] U.S. NUCLEAR REGULATORY COMMISSION, 2010, REGULATORY GUIDE 5.71 - CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

[4-12] Cigre JWG D2/B3/C2-1, 2007, Technical Brochure TB 317 on “Security for Information Systems and Intranets in Electric Power Systems”

[4-13] Cigre WG D2.22, Technical Brochure TB 419 on “Treatment of Information Security for Electric Power Utilities”, June2010.

[4-14] ISO 7498-2: Information processing systems, 1989, Open System Interconnection –
Basic Reference Model – Part 2: Security Architecture

[4-15] IEC Smart Grid Standardization Roadmap, Edition 1.0,
2010 [4-16] PERA Enterprise Model, Gary Rathwell

[4-17] American National Standards Institute (ANSI), International Society of Automation (ISA), “ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration, Part 1: Models and Terminology”

[4-18] J. D. Gilsinn, R. Schierholz, "Security Assurance Levels: A Vector Approach

to Describing Security Requirement," Oct. 2010, Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=906330(last visited 14th May2011)

[4-19] CIGRÉ Working Group WGD2.24 “EMS for the 21st Century - System Requirements” Technical Brochure 452, February 2011.

[4-20] National Institute of Standards and Technology (NIST), 2008, “Guide to Industrial Control Systems (ICS) Security (NIST 800-82)”

[4-21] Department of Homeland Security (DHS), 2006, “Control Systems Cyber Security: Defense in Depth Strategies”

[4-22] US Department of Homeland Security, 2009, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies”. Control Systems Security Program, National Security Division.

[4-23] SINTEF report, 2007, "The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems", Available at: http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/SINTEF%20A1626%20-%20SeSa%20report-final.pdf (last visited 25th April2011)

[4-24] AMI-SEC Task Force and AMI Security Acceleration Project (ASAP), 2009, “AMI Security Implementation Guide V1.01”

[4-25] W32.Stuxnet Dossier, 2011, Nicolas Falliere, Liam O Murchu, Eric Chien Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[4-26] IEC 62443-1, 2008, “Industrial communication networks - Network and system security Part 1 Terminology, concepts and models”, 7 et. sqq.

[4-27] IAEA Nuclear Security Series No. 17: Technical Guidance, Computer Security at Nuclear Facilities, 2011

[4-28] U.S. Nuclear Regulatory Commission (NRC), 2010, “Regulatory Guide 5.71 - Cyber Security programs for Nuclear Facilities”, pp. 35

[4-29] NERC: reliability considerations from the integration of Smart Grid available at http://www.nerc.com/files/SGTF_Report_Final_posted.pdf in particular see defense in depth p 89

[4-30] J.-T. Zerbst, L. Pietre-Cambacedes, Å. Torkilseng and O. Breton, "Graded approach to cyber security for EPUs: Clarifying the security levels and zones concepts," 2011 CIGRE D2 Colloquium, Buenos Aires, Argentina, October 2011

[4-31] IEC 61508 edition 2.0, 2010, “Functional safety of electrical/electronic/programmable electronic safety-related systems”

[4-32] NERC CIP-002 to NERC CIP-009, “Cyber Security Standard of NERC”, 2006, http://www.nerc.com(last visited 27th December 2012)

[4-33] "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security", 2010,

NIST

[4-34] "IT-Grundschutz-Standards", 2008, Federal Office for Information Security of Germany (BSI)

[4-35] "ABB White Paper: Security for Industrial Automation and Control Systems", 2010, ABB [4-36] "Cyber Security Compliant Architecture for the Nuclear Industry" 2011, Invensys

[4-37] ArchiMate® 2.0, 2012, The Open Group

[4-38] “Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)”, Bundesamt für Sicherheit in der Informationstechnik, 2012, Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP_Security_%20Module.pdf?__blob=publicationFile (last visited 27th December 2012)’

[4-39] "Zone principles as Cyber Security architecture element for Smart Grids", 2010, Jens Zerbst, Martin Schaefer, Iiro Rinta-Jouppi

[4-40] Payment Card Industry (PCI) Data Security Standard 2.0, 2010, PCI Security Standard Council

[4-41] L. Pietre-Cambacedes and M. Bouissou, "Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)," Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010), Istanbul, Turkia, pp. 2852-2861, October 2010

[4-42] PERA Enterprise Model, Gary Rathwell, Available at: http://www.pera.net/Pera/PERA_Papers/Levels-4Rs/4r_pres.htm (last visited 27th December 2012)

[4-43] "Data Structures And Algorithms", 1983, A.A. Puntambekar

[5-1] IEC Smart Grid Standardization RoadMap, SMB Smart Grid Strategic Group SG3, Edition 1.0, June 2010.

[5-2] NIST Internal Report 7628, “Guidelines for Smart Grid Cyber Security”, 3 Volumes, The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010.

[5-3] L. Pièrre-Cambacédès, T. Kropp, J. Weiss, R Pellizzoni: “Cybersecurity standards for the electric power industry – a survival kit” – Paper D2-217, CIGRÉ Paris Session 2008, France, August2008.

[5-4] ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, Second edition, 2005.

[5-5] T. Sommestad, M. Ekstedt, P. Johnson, “A probabilistic relational model for security risk analysis,” Computers & Security, vol. 29, no. 6, pp. 659 –679, 2010.

[5-6] N. Falliere, L.O. Murchu, E. Chien “W32.Stuxnet Dossier”, Symantec Security Response, Version 1.4, February 2011.

[5-7] B. Schneier, “Attack trees: Modeling security threats”, Dr. Dobb's Journal, vol. 12, no.24, pp. 21-29, 1999.

[5-8] C.-W. Ten, C.-C. Liu, M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in Proceedings of the IEEE Power Engineering Society General Meeting, pp. 1–8, Tampa, USA, June 2007.

[5-9] S. C. Patel, J. H. Graham, P. A. Ralston, "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements," International Journal of Information Management, vol. 28, no. 6, pp. 483 –491, December2008.

[5-10] S. McLaughlin, P. McDaniel, D. Podkuiko, "Energy theft in the advanced metering infrastructure," in Proceedings of the 4th International Workshop on Critical Information Infrastructure Security (CRITIS'09), Bonn, Germany, 2009.

[5-11] G.-Y. Park, C. K. Lee, J. G. Choi, D. H. Kim, Y. J. Lee, K.-C. Kwon, "Cyber security analysis by attack trees for a reactor protection system," in Proceedings of the Korean Nuclear Society (KNS) Fall Meeting, Pyeong Chang, Korea, October 2008.

[5-12] J. P. McDermott, "Attack net penetration testing," in Proceedings of the 2000 Workshopon New Security Paradigms (NSPW'00), pp. 15 –21, Cork, Ireland, September 2000.

[5-13] S. Pudar, G. Manimaran, C. Liu, "PENET: a practical method and tool for integrated modeling of security attacks and countermeasures," Computers &Security, vol. 28, no. 8, pp. 754–771, May 2010.

[5-14] T. Sommestad, M. Ekstedt, L. Nordström, "Modeling security of power communication systems using defense graphs and influence diagrams," IEEE Transactions on Power Delivery, vol. 24, no. 4, pp. 1801–1808, October 2009.

[5-15] J. McDermott, C. Fox, "Using abuse case models for security requirements analysis," in Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), Phoenix, USA, Dec. 1999, pp.55 –64.

[5-16] G. Sindre, A. L. Opdahl, "Eliciting security requirements with misuse cases,"Requirements Engineering, vol. 10, no. 1, pp. 34 –44, 2005.

[5-17] G. Dondossola, F. Garrone, J. Szanto "Experimental Evaluation of Cyber Intrusions into Highly Critical Power Control Systems" Proceedings of the CIRED 2011 – International Conference on Electricity Distribution, Paper n. 0440, Frankfurt, June 2011.

[5-18] M.-Y. Huang and T. M. Wicks, "A large-scale distributed intrusion detection framework based on attack strategy analysis," in Proceeding of the 1st International Workshop on the Recent Advances in Intrusion Detection (RAID'99), pp. 2433 –248, Louvain-la-Neuve, Belgium, Sep.1998.

[5-19] L. Piètre-Cambacédès, M. Bouissou, "Attack and defense dynamic modeling with BDMP", in Proceedings of the 5th International Conference on Mathematical Methods, Models, and Architectures for Computer Networks

Security (MMM-ACNS-2010), pp. 86– 101, LNCS 6258, St Petersburg, Russia, September 2010.

[5-20] M. Bouissou, J.-L. Bon, "A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes," Reliability Engineering & System Safety, vol. 82, no. 2, pp. 149–163, November 2003.

[5-21] N. Mead, E. Hough, T. Stehney, "Security quality requirements engineering (SQUARE) methodology," Carnegie Mellon University, Tech. Rep. CMU/SEI-2005-TR-009, 2005.

[5-22] S. Evans, D. Heinbuch, E. Kyule, J. Piorkowski, and J. Wallner, "Risk-based systems security engineering: stopping attacks with intention," IEEE Security and Privacy, vol. 2, no. 6, pp. 59–62,2004.

[5-23] Buckshaw, D. L.; Parnell, G. S.; Unkenholz, W. L.; Parks, D. L.; Wallner, J. M. &Saydjari, O. S. Mission Oriented Risk and Design Analysis of Critical Information Systems, Military Operations Research, Vol. 10 No. 2, pp. 19-38, 2005,http://www.innovativedecisions.com/documents/Buckshaw-Parnelletal.pdf.

[5-24] U.S. Nuclear Regulatory Commission (NRC), "Cyber security programs for nuclear facilities," Regulatory Guide 5.71, January 2010.

[5-25] CEN/CENELEC/ETSI "Use Case Management Process — Use Case Collection, Management, Repository, Analysis and Harmonization", Draft Report of the Working Group Sustainable Processes to the Smart Grid Coordination Group - Mandate M/490, November 2012

[5-26] G. Dondossola, F. Garrone, G. Proserpio, C. Tornelli, 2012, "Impact of DER integration on the cyber security of SCADA systems – the Medium Voltage regulation case study". CIRED 2012 Lisbon (PT), 29-30 May 2012

[5-27] G. Dondossola: "Risk Assessment of Information and Communication Systems - Analysis of some practices and methods in the Electric Power Industry", CIGRÉ Electra, No. 239, August2008.

[5-28] ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4210 7.

[5-29] T. Sommestad, M. Ekstedt, H. Holm, 2012, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures". IEEE Systems Journal, 2012

[5-30] IEC/TS 62351-3 ed1.0 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP, 22 June 2007

[5-31] P. Mell, K. Scarfone, S. Romanosky, 2007, ”A complete guide to the common vulnerability scoring system version 2.0”. Forum of Incident Response and Security Teams (FIRST), 2007

[6-1] Robert O’Harrow Jr “Cyber search engine Shodan exposes industrial control systems to new risks” [Washington Post, June 03, 2012] - http://articles.washingtonpost.com/2012-06-03/news/35459595_1_computer-systems-desktop-computers-search-engine

[6-2] An Undirected Attack Against Critical Infrastructure: A case study for improving Your control system Security, http://ics-cert.us-cert.gov/sites/default/files/documents/CaseStudy-002.pdf

[6-3] BSI – aperçu des menaces cybersécurité - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/statistiken/BSI-CS_029.html

[6-4] Trend Micro: Who's really attacking your SCADA, https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf

[6-5] Trend Micro: The SCADA That didn't Cry Wolf, Who's really attacking your SCADA part 2):https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf

[6-6] DHS Cybersecurity Procurement language, http://ics-cert.us-cert.gov/sites/default/files/Procurement_Language_Rev4_100809.pdf

[6-7] DOE Cybersecurity procurement language, http://energy.gov/oe/downloads/cyber-security-procurement-language-control-systems-version-18

[6-8] EPRI Cyber Security Procurement—Application of the Methodology http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002001735

[6-9] EPRI Cyber Security Procurement Methodology http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026562

[6-10] WIB M2784X10 (PCS requirements for vendors)

[6-11] ISO/IEC 27036: Information security for supplier relationships (International standard) [6-12] NISTIR 7628: Guidelines for Smart Grid Cyber Security – Introduction

[6-13] ISO/IEC 62443-3-3:2013: System security requirements and security levels.

[6-14] ISO/IEC TR 27019:2013 Information technology Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

[6-15] Critical Infrastructure Protection (CIP), (NERC, US) and particularly: NERC-CIP-005,

NERC-CIP-006, NERC-CIP-007

[6-16] IEEE P1689, Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access

[6-17] D. K. Holstein, P. Sitbon, “Security requirements in procurement for Electric Power Utilities”, C&ESAR conference, Rennes, France, October 2013.

[6-18] NERC: Guidance for Secure Interactive Remote Access, July
2011 [6-19] VGB S-175 standard

[6-20] ANSSI: méthode de classification et mesures principales pour les installation sindustrielles (french national guideline to be published)

[6-21] ANSSI - Externalisation des systèmes d’information – maîtriser les risques de l’infogérance http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf

[6-22] CPNI Good Practice Guidelines for Process Control and SCADA Security: http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[6-23] DHS/CPNI: Configuring and Managing Remote Access for Industrial Control Systems, November 2011.

[6-24] DoE: 21 Steps to Improve Cyber Security of SCADA Networks

[6-25] EXERA M3958X10 - Cybersécurité des systèmes de contrôle commande

[6-26] CIGRE Electra ELT_244_2 “Security Technologies Guideline - Practical Guidance for Deploying Cyber Security Technology within Electric Utility Data Networks”, June 2009

[6-27] CIGRE Technical Brochure TB419 -”Treatment of Information Security for Electric Power Utilities (EPUs)”, D2.22, June 2010.

[7-1] CIGRÉ Working Group WGD2.01 “Strategic Priorities for Information Systems Issues”, Electra 274, pp 30-33, June 2014.

A.3 Список рисунков

A.4 Список таблиц