УДК 621.3

Защита информации в сетях SMART GRID на основе интеллектуальных технологий

Плешко Д.Ю.
Научные руководители – к.т.н., доцент БЛАДЫКО Ю. В.,
ст. препод. САПОЖНИКОВА А.Г.

Одним из приоритетных направлений развития мировой энергетики является внедрение интеллектуальных энергосетей нового поколения Smart Grid. Однако, как в отечественной, так и в зарубежной литературе, рассматриваются вопросы проектирования и проблемы внедрения энергосетей нового поколения, но не уделяется достаточного внимания вопросам защиты информации в подобных интеллектуальных сетях.

Рассмотрены первые этапы разработки системы защиты информации Smart Grid на основе интеллектуальных технологий – проектирование базы правил на основе онтологии информационной безопасности. Данная онтология информационной безопасности разработана на основе слияния двух других онтологий предметной области – Gridpedia и Онтологии кибербезопасности в энергетике.

В процессе слияния осуществлена перегруппировка основных классов онтологий, а также добавлены новые классы и свойства. Подобный подход позволил не выполнять работу с нуля, а учесть и использовать разработки других специалистов в данной предметной области. Интеллектуальная энергосеть; система защиты информации; онтология; информационные риски; база правил.

Впервые Smart Grid как термин появился в западных странах, где он применялся для именования контроллеров, предназначенных для управления режимом работы и синхронизации автономных ветрогенераторов, отличительной чертой которых является нестабильная частота и напряжение, с электрической сетью.

Впоследствии с помощью данного термина стали обозначаться микропроцессорные счетчики электроэнергии, способные накапливать, обрабатывать, оценивать информацию, а также передавать ее по специальным каналам связи, в том числе через сеть Интернет. В последние годы термин Smart Grid используется в тех областях, где используются системы сбора и обработки информации, а также мониторинга состояния оборудования в энергетике.

Технология Smart Grid наиболее интенсивно развивается и распространяется в США, Дании, Швеции, Испании, Великобритании и КНР. Однозначного определения, характеризующего данную технологию, пока нет, существует только ряд требований, которым сеть должна отвечать.

В данной статье под интеллектуальной сетью понимается совокупность подключённых к генерирующим источникам и электроустановкам потребителей, программно-аппаратных средств, а также информационно-аналитических и управляющих систем, обеспечивающих надёжную и качественную передачу электрической энергии от источника к приёмнику в нужное время и в необходимом количестве.

В данной работе предлагается использовать интеллектуальный подход к проектированию системы защиты информации для сети Smart Grid, так как он позволяет реализовать основные принципы построения системы защиты: постоянство, надежность, системность, комплексность, адекватность, гибкость, непрерывность.

А также позволит реализовывать упреждающую стратегию защиты, в основу которой должна быть положена способность полной адаптации к любым изменениям условий функционирования сети Smart Grid.

Интеллектуальный подход содержит следующие этапы:

– разработка базовой онтологии, разработка онтологии предметной области;

– разработка модели типовых технологических процессов, аксиологических (ценностных) моделей.

– проектирование базы знаний;

– разработка базы прецедентов;

– создание интеллектуальной системы поддержки и принятия решений.

Целью данной работы является выполнение первых трех из всех описанных выше этапов и получение, в результате, базы знаний интеллектуальной сети Smart Grid, для проектирования которой потребовалось разработать онтологию информационной безопасности интеллектуальной сети Smart Grid.

Впервые понятие онтологии сформулировано Т. Грубером. Он предлагал использовать это понятие для представления знаний в конкретной предметной области в декларативной форме. В широком смысле, онтология – это база знаний специального вида, или «спецификация концептуализации» предметной области. Это означает, что в рассматриваемой предметной области на основе классификации базовых терминов выделяются основные понятия (концепты) и устанавливаются связи между ними (концептуализация).

Онтология имеет разные формы представления: графический вид или формальная онтология (представлена с помощью формального языка).

Процесс представления онтологии носит название процесса спецификации онтологий. Онтология определяет общий словарь для ученых, которым нужно совместно использовать информацию в предметной области. Она включает машинно-интерпретируемые формулировки основных понятий предметной области и отношения между ними.

Онтологический подход к описанию энергетических систем Smart Grid сегодня уже применяется. Есть уже созданные онтологии сетей Smart Grid. Наиболее полной онтологией является онтология Gridpedia. Однако в таких онтологиях вопросы защиты информации либо не рассматриваются, либо отходят на второй план.

Поэтому была разработана рассмотренная ниже онтология информационной безопасности интеллектуальной сети Smart Grid. Данная онтология получилась в результате слияния двух онтологий: Gridpedia и онтологии кибербезопасности в энергетике (онтология Ворожцовой).

Gridpedia может быть использована для достаточно подробного описания Smart Grid как энергосистемы. Онтология кибербезопасности в энергетике позволяет описать систему с точки зрения информационной безопасности. Таким образом, к существующим классам и свойствам Gridpedia были добавлены классы и свойства из онтологии Ворожцовой.

К онтологии информационной безопасности были предъявлены определенные требования, которым она должна отвечать с точки зрения процесса проектирования Smart Grid.

Для обеспечения соответствия этим требованиям основные классы и свойства онтологии были перегруппированы. На рисунке 1показан один из классов онтологии – класс Data (данные) и иерархия его подклассов из разработанной онтологии кибербезопасности Smart Grid.

В качестве следующего шага была проведена работа по разработке базы правил на основе онтологии.

С позиции информационной безопасности, наиболее важными аспектами Smart Grid являются:

– менеджмент – защита конфиденциальной информации с точки зрения управления персоналом – рассматриваются угрозы, связанные с преднамеренными либо случайными действиями сотрудников Smart Grid;

– приложения и базы данных – защита от угроз, возникающих на уровне приложений и баз данных;

– сеть – защита от угроз, которые могут возникнуть в связи с использованием LA - и WA -сетей, в том числе угроз из сети Интернет;

– мобильные устройства – защита от угроз, связанных с использованием GSM-сетей и мобильных телефонов.

Для анализа угроз и разработки мер противодействия выявленным угрозам были выбраны два базовых метода: SREP и CORAS, разработанные в соответствии с международным стандартом ISO/IEC 2700.

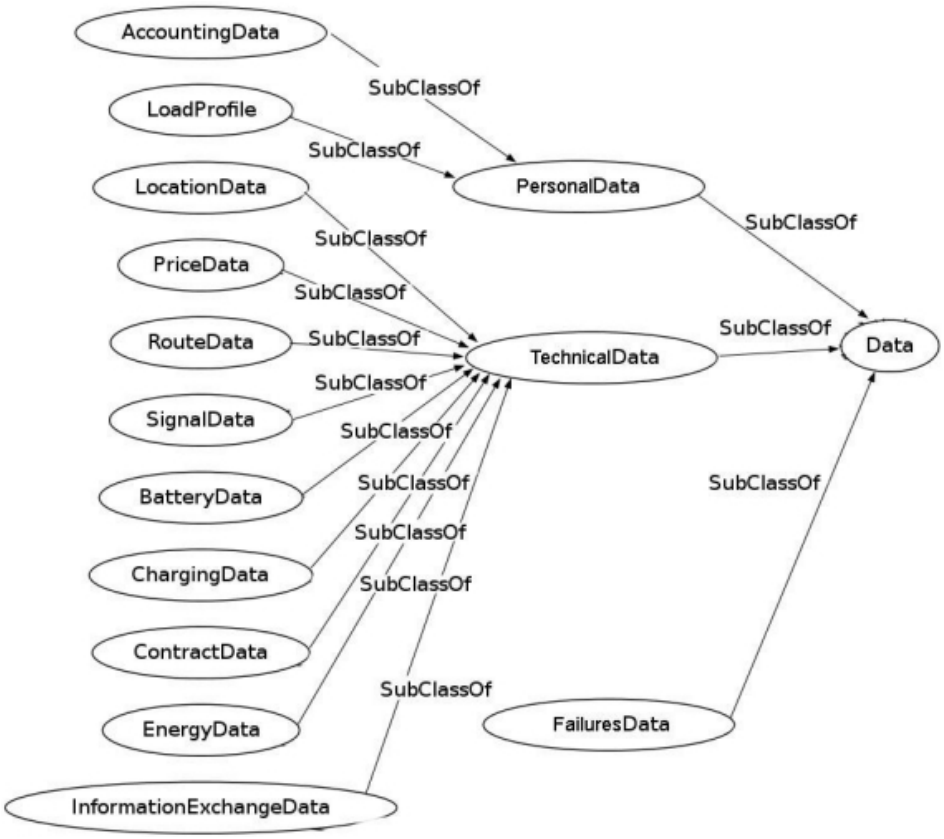

Рисунок 1 – Класс Data и иерархия его подклассов

Данные методы выбраны как наиболее подходящие для достижения поставленных целей. С помощью SREP осуществлен анализ эффективности системы защиты с точки зрения менеджмента и мобильных устройств, с помощью CORAS – анализ эффективности системы защиты с точки зрения приложений, баз данных и сети.

Оценка возможного риска происходила в соответствии с методологией, предложенной в стандарте ISO/IEC 27005.

В соответствии с разработанной онтологией были выделены три вида информационных ресурсов, подлежащих защите:

– персональные данные пользователей Smart Grid;

– техническая информация, поступающая от клиентов сети;

– информация о системных сбоях и ошибках, которые происходят при работе сети.

К требованиям, которые должна реализовывать система защиты, были отнесены:

– предотвращение неавторизованного раскрытия защищаемой информации;

– обеспечение постоянного доступа пользователей к защищаемой информации;

– предотвращение несанкционированного изменения защищаемой информации.

В результате исследования были выделены 23 угрозы информационной безопасности Smart Grid. В том числе 6 угроз на уровне менеджмента, 7 – на уровне приложений и баз данных, 7 – на уровне сети и 3 – на уровне мобильных устройств.

Для устранения указанных угроз выделены 23 требования к информационной безопасности Smart Grid. Перечень основных требований содер-жит 8 требований на уровне менеджмента, 6 – на уровне приложений и баз данных, 5 – на уровне сети и 4 – на уровне мобильных устройств.

В результате работ был описан процесс проектирования базы правил системы поддержки принятия решений по обеспечению информационной безопасности сети Smart

Grid. В качестве первого этапа разработана онтология, позволяющая описать интеллектуальную сеть Smart Grid с точки зрения информационной безопасности.

Для этого проведен анализ существующих онтологий; выбраны две онтологии, наиболее близко подходящие для решения поставленной задачи. Данные онтологии объединены и перестроены таким образом, чтобы получившаяся онтология отвечала предъявляемому к ней требованию – описанию интеллектуальной сети Smart Grid с точки зрения информационной безопасности. Проведен анализ угроз информационной безопасности, разработаны требования к системе информационной безопасности интеллектуальной сети, предложены контрмеры, позволяющие уменьшить риски осуществления угроз информационной безопасности. В результате данных действий спроектирована база знаний, необходимая для разработки системы поддержки и принятия решений. Данная система должна обеспечить информационную защищенность интеллектуальной сети Smart Grid.

Таким образом, данная работа, является первым шагом на пути создания системы защиты информации интеллектуальной сети Smart Grid, основанной на применении интеллектуальных технологий.