Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. Том 2 (68). 2016 г. № 3. С. 49–57.

УДК 004.056.5

КОМПЛЕКСНЫЙ ПОДХОД К МОДЕЛИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Дячук В. С.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: bolek61@mail.ru

В статье рассматриваются основы моделирования систем защиты данных в сфере управления и контроля электроэнергетикой. Проанализированы принципы, подходы и методы создания комплексной системы защиты информации на энергообъектах. Предложен комплексный подход к моделированию системы информационной безопасности с учетом многоуровневой организации информационного обмена на энергообъектах.
Ключевые слова: информационная безопасность, объект электроэнергетики, моделирование, угрозы, нарушения, контроль, комплексная система защиты информации.

ВВЕДЕНИЕ

Безопасность объектов электроэнергетики является одним из определяющих факторов полноценного и полноправного проживания граждан на территории Российской Федерации. В свою очередь, создание модели комплексной системы защиты информации является первоочередным и необходимым требованием к обеспечению устойчивого и надежного барьера от хищения, деформации и несанкционированного присвоения информации с учетом многоуровневой организации информационного обмена на энергообъектах.

Современное положение дел с энергообеспечением Республики Крым в аспекте проблематики информационной безопасности систем учета и контроля электроэнергетики не вызывает сомнений [1, 2].

Создание устойчивой и надежной системы информационной безопасности заключается в моделировании системы в наиболее приближенных к реальности условиях. Целью моделирования различных объектов является возможность изучить проблему многогранно и выявить недостатки и уязвимости системы, а также предложить наиболее подходящие варианты для решения поставленных задач.

В работе профессора Вишневского В. М. «Теоретические основы проектирования компьютерных сетей» процесс моделирования определен как «замещение одного объекта (оригинала) другим (моделью) и фиксация или изучение свойств оригинала путем исследования свойств модели» [3]. Замещение производится с целью упрощения, удешевления или изучения свойств оригинала. Моделирование системы состоит в построении некоторого ее образа, соответствующего (с точностью до целей моделирования) исследуемой системе, и получения с помощью сформированной модели необходимых характеристик реальной системы.

Основы информационного обмена на объектах электроэнергетики рассматривались ранее в части структуры основных уровней организации обмена данными согласно МЭК–61850 [4]. Последующие научные исследования обусловлены необходимостью разработки комплексного подхода к созданию современной системы защиты данных на объектах электроэнергетики Республики Крым.

Цель исследования заключается в определении комплексного подхода к созданию модели защиты данных на энергообъектах с учетом многоуровневой организации информационного обмена на энергообъектах.

ОСНОВНОЙ МАТЕРИАЛ

Процесс моделирования системы целесообразно начинать с определения научно-методологических основ построения комплексной системы защиты информации (далее КСЗИ). Научно-методологические основы – это множество принципов, подходов и методов, необходимых для определения и исследования проблем системы комплексной защиты, анализа её уязвимостей и потенциальных угроз в целях разработки оптимальных механизмов защиты и управления механизмами защиты в процессе их функционирования [5].

Следуя вышеуказанному определению, к основным составляющим научно-методологическим основам относят принципы, подходы и методы (рис. 1).

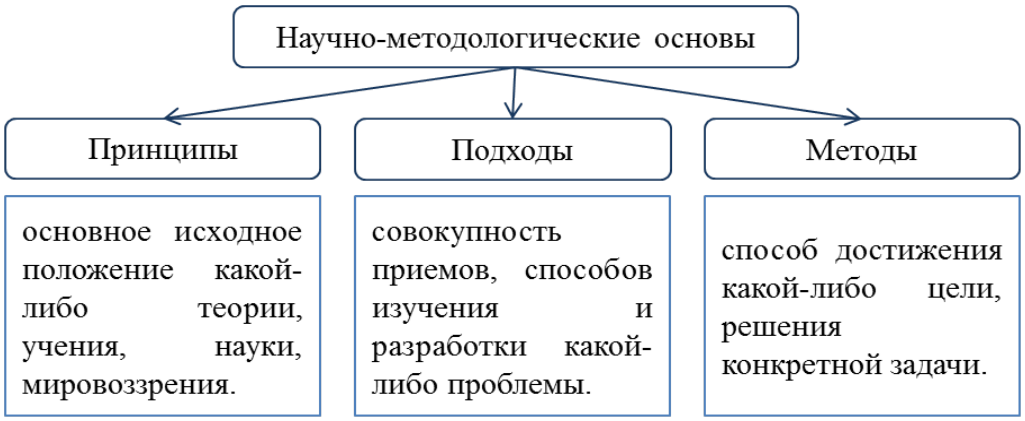

Рис. 1. Научно-методологические основы моделирования системы комплексной защиты информации.

Источник: составлено автором по материалам [5].

К основным принципам построения комплексной системы защиты информации относят:

1) принцип законности;
2) принцип полноты ЗИ;
3) принцип обоснованности ЗИ;

4) принцип распределения прав доступа;
5) принцип участия субъектов защиты;
6) принцип персональной ответственности;
7) принцип следования руководству по ЗИ;
8) принцип предупредительных мер по ЗИ [6].

Каждый из принципов имеет свои особенности, однако именно их совокупность создает полноценное обоснование применения тех или иных подходов к моделированию КСЗИ.

Подходы к моделированию комплексной системы защиты информации позволяют при помощи научных, научно-технических и организационных мероприятий, специальных средств и методов создать максимально эффективную, полноценно функционирующую систему обеспечения безопасности информации и информационного обмена [7].

В части защиты данных наиболее приемлемым является системно-концептуальный подход, основанный на эмпирических, экспериментальных и теоретических исследованиях.

Понятие системности является основой системно-концептуального подхода (далее – СКП) в рамках защиты информации (рис. 2).

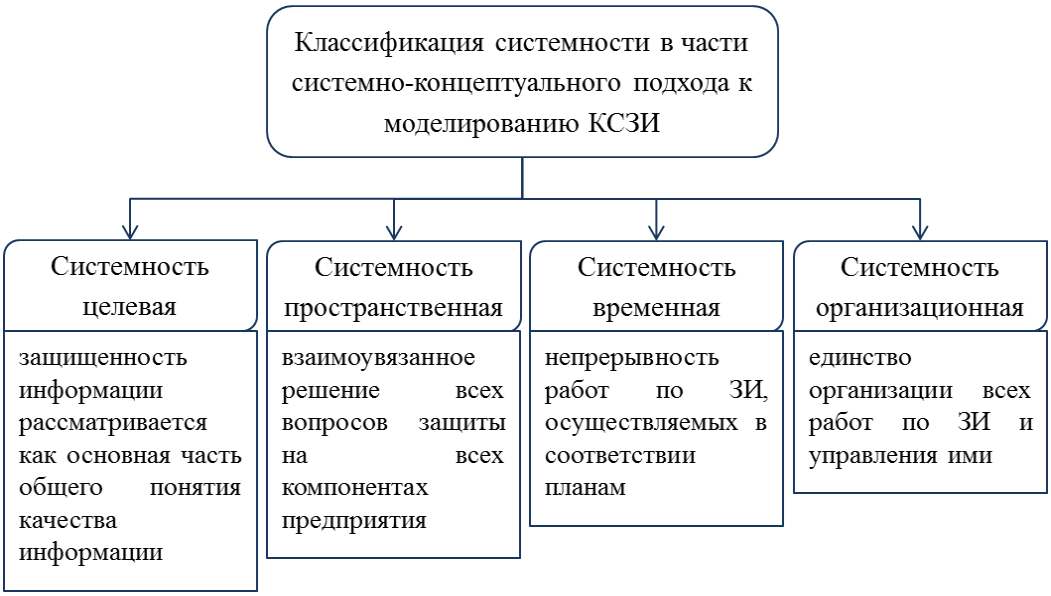

Рис. 2. Классификация системности в части системно-концептуального подхода к моделированию КСЗИ.

Источник: составлено автором по материалам [8].

Понятие концептуальности в части системно-концептуального подхода к моделированию КСЗИ заключается в разработке общей концепции как системы научно обоснованных взглядов, согласованности с единым замыслом,

конструктивным принципом решения поставленных задач, необходимых для организации полноценного функционирования комплексной системы защиты информации [8].

Комплексный подход подразумевает изучение системы в целом, а не отдельных её составляющих, в этом и состоит его главная задача. Создание системы защиты информации по основным положениям комплексного подхода начинается с определения её компонентов: входных данных, ресурсов, окружающей среды, назначений и функций, критериев эффективности.

Входные элементы – это те элементы, для обработки которых создается система. В случае построения КСЗИ входными элементами выступают угрозы безопасности данных, возможные на данном объекте.

К ресурсам следует отнести методы, средства и инструменты, необходимые для создания и полноценного функционирования КСЗИ.

Окружающая среда в моделировании систем защиты информации подразумевает иные системы, с которыми возможно взаимодействие КСЗИ, здесь рекомендуется устанавливать границы областей таких систем и режимы их совместного функционирования (передача сигналов по кабельной линии и т. п.) [9].

Функциональная зависимость элементов в системе должна ориентироваться на цель, с которой данная система создается. Здесь важны точность и конкретность поставленной цели, состоящей из назначения и функций системы.

За определением подхода к моделированию системы следует выбор метода моделирования СЗИ, позволяющий эффективно решать задачи анализа и синтеза больших систем защиты самой различной природы и архитектуры, а также управления процессами их функционирования.

В целях установления метода моделирования КСЗИ для начала определяют класс модели (рис. 3).

Рис. 3. Классификация моделей систем защиты информации.
Источник: составлено автором по материалам [10].

Все модели могут быть разделены на аналитические и статистические: первые представляются в виде некоторой совокупности аналитических и/или логических

зависимостей и позволяют определять необходимые характеристики путем проведения вычислений по указанным зависимостям, а при статистическом моделировании СЗИ представляется в виде некоторого аналога, отражающего для определяемых характеристик зависимости реальной системы защиты. Моделируемые СЗИ подразделяются на детерминированные и стохастические (определены все строгие зависимости, а также существенно влияют случайные факторы). Модели систем защиты в зависимости от цели моделирования подразделяются на общие (изучение обобщенных характеристик СЗИ) и частные (определение локальных характеристик СЗИ) [10].

На функционирование системы защиты информации так или иначе влияют случайные факторы, следовательно, большинство моделей КСЗИ стохастичны. Также модель защиты информации на объектах электроэнергетики имеет локальное назначение и зависимость. Таким образом, второй и третий классы моделей исключаются из классификации, и достаточно иметь в виду всего два варианта моделей: аналитические частные и статистические частные.

Модель защиты информации на объекте электроэнергетики будет носить характер аналитической стохастической частной модели.

Методы, применяемые для моделирования системы защиты информации, делятся на три вида: вербальные, физические и математические [11].

Вербальная модель заключается в описании объекта на естественном или профессиональном языках. Данный метод моделирования позволяет исследовать связи между элементами системы только на качественном уровне.

В свою очередь физическая модель представляет собой вещественный аналог реальной системы, над которым можно ставить экспериментальные опыты и получать количественную меру взаимодействия между данными опытами и их результатами. Так, методы структурирования являются развитием формального описания, распространяющимся на организационно-технические системы. Согласно учебному пособию по информационной безопасности Семененко В. А., «использование этих методов позволяет представить архитектуру и процессы функционирования сложной системы в виде, удовлетворяющем следующим условиям: полнота отражения основных элементов и их взаимосвязей; простота организации элементов и их взаимосвязей; гибкость – простота внесения изменений в структуру и т. д.» [12]. Однако данный метод моделирования требует больших затрат в реализации как материальных, так трудовых и временных.

Математическое моделирование предусматривает создание и исследование реальных процессов и объектов при помощи математического аппарата. Математическая модель рассматривается как совокупность аналитических зависимостей выходных потоков информации от входных, функций и уравнений для моделирования динамически изменяющихся процессов в системе защиты информации, статистических характеристик реакций системы на воздействия случайных факторов [13].

Каждый из рассмотренных методов моделирования не дает максимальную эффективность в создании наиболее оптимальных моделей системы защиты информации, поэтому рационально применение методов в совокупности. Обычно

используется комбинация вербального, физического и математического моделирования, при этом сам процесс моделирования начинается с описания модели на вербальном уровне, создается образное представление об объекте и его словесное описания. Далее, если есть возможность создать физическую модель, то лучше прибегнуть именно к ней, это позволит максимально точно исследовать физические свойства объекта. Если же по каким-либо причинам нет такой возможности, то стоит использовать математическую модель с элементами физической (моделируя отдельные узлы/элементы системы, описание которых не поддаётся формализации).

Таким образом, при условии высокой трудоемкости, материалоемкости и больших временных затрат при построении сложной модели системы защиты информации для упрощения процесса моделирования целесообразна детализация отдельных ключевых элементов и связей между ними [14].

Для определения элементов в случае построения КСЗИ на объектах электроэнергетики целесообразно обратиться к Федеральному закону Российской Федерации «Об электроэнергетике», определяющему такие основные понятия, как электроэнергетика, субъекты электроэнергетики, потребители электрической и тепловой энергии, объекты электросетевого хозяйства, услуги по передаче электрической энергии, услуги по оперативно-диспетчерскому управлению в электроэнергетике [15].

Электроэнергетику следует рассматривать как отрасль экономики, состоящую из комплекса экономических отношений, а также как систему информационного обмена, состоящую из центров оперативно-диспетчерского управления, коммерческого учета, а также потребителей.

К субъектам электроэнергетики относятся лица, осуществляющие деятельность в сфере электроэнергетики. В рамках проектирования КСЗИ задействуются субъекты, регулирующие качественные и количественные показатели подачи электрической энергии, а также участвующие в оперативно-диспетчерском управлении.

Потребители электроэнергии в системе защиты информации играют роль также и потребителей информации, здесь представлены лица, приобретающие электрическую и тепловую энергию для собственных бытовых и (или) производственных нужд. Сюда же следует отнести субъекты рынка электрической энергии, т. к. их роль в КСЗИ идентична роли потребителей электроэнергии.

Объектами электросетевого хозяйства согласно анализируемому Федеральному закону являются линии электропередачи, трансформаторные подстанции, распределительные пункты и прочее специализированное оборудование. В рамках моделирования КСЗИ объекты электросетевого хозяйства являются основными объектами, включающими системы передачи, обработки и хранения данных.

Услуги по оперативно-диспетчерскому управлению в электроэнергетике в части моделирования КСЗИ описывают функциональные зависимости и назначения по передаче данных в системе. Данные услуги включают комплекс мер по централизованному управлению технологическими режимами работы технических устройств электростанций (коммутаторы, контроллеры и др.), электрических сетей

и энергопринимающего оборудования потребителей электрической энергии с управляемой нагрузкой (датчики и счетчики), осуществляемых в целях обеспечения надежного энергоснабжения и качества электрической энергии, соответствующих техническим регламентам и иным обязательным требованиям [16].

Таким образом, согласно требованиям международных стандартов (МЭК–61850 и др.) и Федерального Закона «Об электроэнергетике» в соответствии с методикой моделирования систем защиты информации к основным элементам системы информационного обмена в сфере электроэнергетики следует отнести, прежде всего, потребителей и субъектов электроэнергетики, объектов электросетевого хозяйства, а также услуги по оперативно-диспетчерскому управлению, определяющие функциональную связь между ними (рис. 4).

Рис. 4. Основные элементы моделирования КСЗИ в электроэнергетике согласно ФЗ № 35.

Источник: составлено автором по материалам [15].

Таким образом, подводя итоги, следует заключить, что при формировании многоуровневой организации информационного обмена на энергообъекте образуются три уровня (станции) передачи и обработки данных, требующих разработки комплексного подхода к моделированию системы мер информационной безопасности, а именно:

1) уровень потребителя;
2) уровень коммерческого учета электроэнергии;
3) уровень технического учета электроэнергетики.

ВЫВОДЫ

В результате проведенного анализа сформированы основные критерии комплексного подхода к моделированию системы защиты информации на объектах электроэнергетики, состоящие в следующем:

1. следовании принципам защищаемой информации (законности, полноты ЗИ, обоснованности ЗИ, распределения прав доступа, участия субъектов защиты, персональной ответственности, следования руководству по ЗИ, предупредительных мер по ЗИ);

2. соблюдении условий системности (целевой, программной, временной и организационной);

3. представлении методики в комбинации вербального, физического и математического моделирования;

4. принятии условий использования аналитической стохастической частной модели;

5. принятии начального этапа создания системы защиты информации с определения потребителей, объектов и субъектов электроэнергетики, а также связей между ними.

Полученные в ходе данного исследования результаты могут быть основой для дальнейших научных исследований в сфере обеспечения информационной безопасности объектов электроэнергетики.

Список литературы

1. Бойченко О. В., Дячук В. С. Проблемы информационной безопасности объектов электроэнергетики Республики Крым // Экономика Крыма. № 4. 2014. С. 156–161.
2. Бойченко О. В., Дячук В. С. Безопасность энергообъектов Республики Крым: предпосылки становления и развития // Труды I Международной научно-практической конференции «Проблемы информационной безопасности». 2015. С. 53–54.
3. Вишневский В. М. Теоретические основы проектирования компьютерных сетей. 2003. 512 с.
4. Бойченко О. В., Дячук В. С. Структура информационного обмена на энергообъекте согласно МЭК–61850 // Журнал «Молодой ученый: вызовы и перспективы»: по материалам XI международной заочной научно-практической конференции. № 9 (11). 2016. С. 508–515.
5. Гришина Н. В. Организация комплексной системы защиты информации. М., 2007. 254 с.
6. Гришина Н. В., Мецатунян М. В., Партыка Т. Л. Принципы организации комплексной системы безопасности коммерческого банка. М., 2008. С. 85–90.
7. Алиев Т. И. Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363 с.
8. Грибунин В. Г., Чудовский В. В. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. Заведений. М., 2009. 416 с.
9. Сущность и задачи комплексной системы защиты информации // Система «Моя библиотека» [Электронный ресурс]. URL: http://mybiblioteka.su/6–23084.html (дата обращения 28.09.2015 г.).
10. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов // Технические науки: теория и практика: материалы III международной научной конференции 2016. С. 6–9.
11. Моделирование КСЗИ. Методы моделирования систем защиты информации и их характеристика [Электронный ресурс]. URL: http://www.audit–ib.ru/complete–protection/information–security/modelling
12. Семененко В. А. Информационная безопасность: учебное пособие. М., 2010. 276 с.
13. Моделирование процессов комплексной системы защиты информации // Система «razlib.ru» [Электронный ресурс]. URL: http://www.razlib.ru/kompyutery_i_internet/organizacija_kompleksnoi_sistemy_zashity_informacii/p7.php
14. Аманжолова С. Т., Ускенбаева Р К. Комплексный метрический подход к организации системы информационной безопасности РКС // Труды II Международной научно–практической конференции «Информационно–инновационные технологии: интеграция науки, образования и бизнеса». 2011.

15. Об электроэнергетике Федеральный закон от 26 марта 2003 № 35–ФЗ (с изменениями на 30 марта 2016 года) // СПС КонсультантПлюс

16. Макаров А. А. Электроэнергетика России в период до 2030 года. Контуры желаемого будущего. М., 2007. 184 с.

Статья поступила в редакцию 10.10.2016