Раздел II. Сетевая безопасность

УДК 004.735

И.Н. Пащенко, В.И. Васильев, М.Б. Гузаиров

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ SMART GRID НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ: ПРОЕКТИРОВАНИЕ БАЗЫ ПРАВИЛ

Одним из приоритетных направлений развития российской и, в целом, 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. Помимо разработки онтологии информационной безопасности интеллектуальных сетей Smart Grid для формирования базы правил были использованы методы SREP и CORAS, разработанные в соответствии с требованиями международных стандартов ISO/IEC 27000. С их помощью разработаны таблицы основных угроз информационной безопасности Smart Grid-сетей, требований к системе защиты информации интеллектуальных сетей и контрмер для снижения риска осуществления рассматриваемых угроз информационной безопасности. В качестве подтверждения эффективности предлагаемых контрмер показана возможность управления рисками информационной безопасности в сетях Smart Grid с использованием предлагаемого набора контрмер.

Интеллектуальная энергосеть; система защиты информации; онтология; информационные риски; база правил.

I.N. Pashchenko, V.I. Vasilyev, M.B. Guzairov

SMART GRID SECURITY SYSTEM ON THE BASIS OF INTELLIGENT TECHNOLOGIES: RULE BASE DESIGN

The important stage in development of modern Russian and the whole world energy technology is implementing the new generation of intelligent energy nets Smart Grids. However, both national and foreign literature focuses on the Smart Grid design and implementing issues, but insufficient attention is paid to information security issues in these intelligent nets. This paper describes the first stages of Smart Grid security system design based on intelligent approach – rule base design on the basis of Smart Grid security ontology. This information security ontology was developed on the basis of two domain ontologies junction – Gridpedia and Cybersecurity ontology in energetics. There was a regrouping of the main ontologies classes and adding new classes and properties during the junction process. Such approach allowed us not to do all the work from the very beginning, but to do it with the accordance to developments of other specialists. Except the Smart Grid information security ontology development, two methods were used for rule base form-

ing. These methods were developed according to the international group of standards ISO/IEC 27000. They were used for design of the tables containing basic Smart Grid information security threats, security system requirements and security controls allowing decreasing risks of security threats realization. To prove the efficiency of proposed security countermeasures, the possibility of risk management in Smart Grid nets with use of offered countermeasures set is shown.

Intelligent energy net; information security system; ontology; information risks; rule base.

В "Энергетической стратегии России на период до 2030 года" [1] под первым пунктом стоит задача разработки и внедрения в эксплуатацию в Российской Федерации интеллектуальных сетей (Smart Grid).

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 [2]. 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 [3].

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 [4]. При этом перечень данных требований в разных странах различен. Версия Министерства энергетики США приведена в [5], а точка зрения, которой придерживаются в Российской Федерации, – в [6] и [7].

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 России большое внимание уделяется различным пилотным проектам, направленным на создание сетей Smart Grid [8]. Одной из актуальных проблем в области создания интеллектуальных сетей является проблема обеспечения их информационной безопасности.

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 [9]:

1. Разработка базовой онтологии, разработка онтологии предметной области.
2. Разработка модели типовых технологических процессов, аксиологических (ценностных) моделей.
3. Проектирование базы знаний.
4. Разработка базы прецедентов.
5. 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 (T. Gruber) [10]. 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. Вопросы онтологического моделирования рассматривались в работах Т. Грубера (Gruber T.), Н. Гуарино (Guarino N.) и др., а в нашей стране – Т.А. Гавриловой, Ю.А. Загорулько, Л.А. Калиниченко, Л.В. Массель и др. [11].

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.

Таким образом, основными преимуществами онтологий являются [12]:

- *системность* – онтология представляет целостный взгляд на предметную область;
- *единообразие* – материал, представленный в единой форме гораздо лучше воспринимается и воспроизводится;
- *научность* – построение онтологии позволяет восстановить недостающие логические связи во всей их полноте.

К сожалению, при разработке новых и использовании существующих онтологий возникает множество трудностей. В работе [13] выделяются, в частности, следующие:

- отсутствие стандартизованных идентифицирующих особенностей, которые характеризовали бы онтологии с точки зрения пользователя;
- разный уровень детализации онтологий, находящихся на одном сервере;
- отсутствие web-сайтов, использующих одинаковую логическую структуру и предоставляющих релевантную информацию об онтологиях;
- поиск подходящих онтологий сложен, занимает много времени, а также часто безрезультатен.

Онтология – формальное явное описание понятий в рассматриваемой предметной области (классов, иногда их называют понятиями), свойств каждого понятия, описывающих различные свойства и атрибуты понятия (слотов (иногда их называют ролями или свойствами)), и ограничений, наложенных на слоты (фацетов, иногда их называют ограничениями ролей). Онтология вместе с набором индивидуальных экземпляров классов образует базу знаний [14].

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

Поэтому нами была разработана рассмотренная ниже онтология информационной безопасности интеллектуальной сети Smart Grid. Данная онтология получилась в результате слияния двух онтологий: Gridpedia и онтологии кибербезопасно-

сти в энергетике (онтология Ворожцовой [15]). 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 рис. 1 показан один из классов онтологии – класс Data (данные) и иерархия его подклассов из разработанной онтологии кибербезопасности Smart Grid.

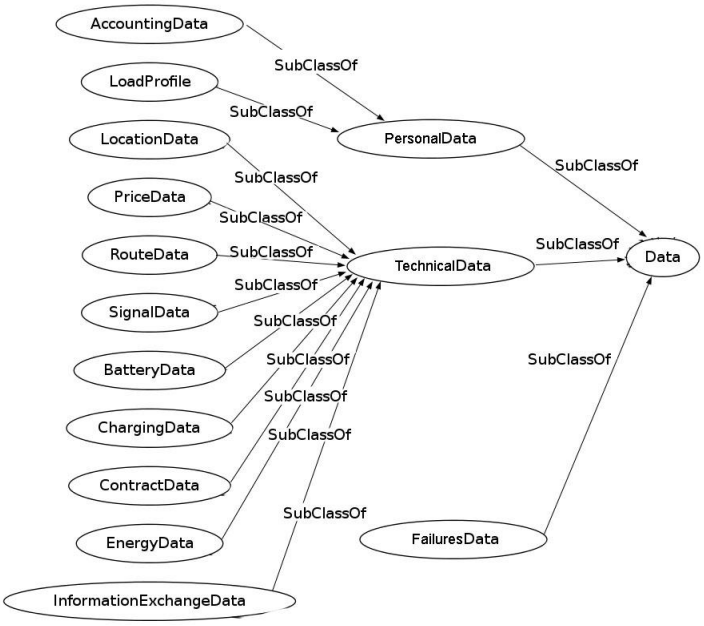

Рис. 1. Класс Data и иерархия его подклассов

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 LAN- и WAN-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 [16] и CORAS [17], разработанные в соответствии с международным стандартом ISO/IEC 27001 [18].

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 (класс Risk) происходила в соответствии с методологией, предложенной в стандарте ISO/IEC 27005 [19].

В соответствии с разработанной онтологией были выделены три вида информационных ресурсов, подлежащих защите (рис. 1):

1. Персональные данные пользователей Smart Grid (PersonalData).
2. Техническая информация, поступающая от клиентов сети (TechnicalData).
3. Информация о системных сбоях и ошибках, которые происходят при работе сети (FailuresData).

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

- предотвращение неавторизованного раскрытия защищаемой информации (Confidentiality);
- обеспечение постоянного доступа пользователей к защищаемой информации (Availability);
- предотвращение несанкционированного изменения защищаемой информации (Integrity).

В результате исследования были выделены 23 угрозы (Threat) 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. Фрагмент разработанной таблицы угроз представлен в табл. 1.

Таблица 1

Угрозы безопасности Smart Grid

№	Угрозы
Менеджмент	
T1	Неавторизованное раскрытие/изменение/лишение доступа к персональным данным/техническим данным/данным об отказах в результате неверного распределения прав доступа к системам Smart Grid
T2	Неавторизованное раскрытие/изменение/лишение доступа к персональным данным в результате сбоя/не произведения обновления систем, функционирующих в Smart Grid
Приложения и базы данных	
T7	SQL-инъекции в систему информирования клиентов, SCADA-систему, платежную систему
T8	XSS-атаки на систему информирования клиентов
Сеть	
T14	Перехват пакетов системы информирования клиентов
T15	Сканирование портов
Мобильные устройства	
T21	Неавторизованное раскрытие/изменение персональных данных/ технических данных/данных об отказах в результате извлечения информации из утерянного/украденного устройства
T22	Неавторизованное раскрытие/изменение персональных данных/ технических данных/данных об отказах в результате использования списанного/неверно обновленного устройства

Для устранения указанных угроз выделены 23 требования (Requirement) к информационной безопасности Smart Grid. Перечень основных требований содержит 8 требований на уровне менеджмента, 6 – на уровне приложений и баз данных, 5 – на уровне сети и 4 – на уровне мобильных устройств. Фрагмент разработанной таблицы требований информационной безопасности представлен в табл. 2.

Таблица 2

Требования к безопасности

№	Требование
Менеджмент	
SR1	Должна быть задокументирована персональная ответственность за выполнение всех действий всеми пользователями Smart Grid
SR2	Должны быть четко указаны роли пользователей Smart Grid
Приложения и базы данных	
SR9	Вводимые данные, используемые в SQL-запросах к системе информирования клиентов/SCADA/платежной системе, должны тщательно проверяться
SR10	Вводимые данные на сайте системы информирования клиентов должны тщательно проверяться
Сеть	
SR15	Содержание передаваемых пакетов должно защищаться и верифицироваться
SR16	Должны быть разработаны мандатные управленческие функции для системы информирования клиентов/SCADA-системы
Мобильные устройства	
SR20	Должно быть обеспечено безопасное удаление важной информации
SR21	Должны быть разработаны действия, которые необходимо применять в случае списания устройства

Для того чтобы снизить вероятность реализации угроз злоумышленниками до приемлемого уровня, были предложены 30 контрмер (Control). Список основных контрмер содержит 8 контрмер на уровне менеджмента, 10 – на уровне приложений и баз данных, 8 – на уровне сети и 4 – на уровне мобильных устройств. Фрагмент разработанной таблицы контрмер представлен в табл. 3.

Таблица 3

Контрмеры

№	Контрмера
Менеджмент	
C1	В соглашениях о неразглашении, контрактах о приеме на работу, контрактах с клиентами должны быть указаны пункты, в которых ясно указываются персональные обязанности по обеспечению безопасности. Каждый пользователь должен ознакомиться с предъявляемыми к нему требованиями и расписаться в соответствующем журнале о том, что он ознакомлен с ними
C2	Все работники Smart Grid (менеджеры, администраторы SCADA, администраторы Smart Grid) должны проходить обязательные тренинги и регулярно оповещаться обо всех изменениях в политиках и процедурах безопасности, относящихся к их обязанностям
Приложения и базы данных	
C9	Использовать фильтрацию входных данных в системе информирования клиентов/SCADA-системе/платежной системе
C10	Использовать межсетевой экран веб-приложений для сайта системы информирования клиентов
Сеть	
C19	Использовать шифрование при формировании и передаче пакетов
C20	Использовать межсетевой экран для серверов системы информирования клиентов/SCADA-системы
Мобильные устройства	
C27	Использовать политику информационной безопасности Google Apps Device Policy
C28	Разработать корпоративную политику списания мобильных устройств

Полные перечни угроз, требований и контрмер представлены в статье [20].

В табл. 4 приведены правила, устанавливающие связь рассмотренных выше угроз, требований и необходимых контрмер.

Таблица 4

База правил

Уровень	Угрозы	Требования	Контрмеры
Менеджмент	T1	SR2, SR3, SR4, SR5, SR6	C3, C5, C4, C6
	T2, T3	SR1, SR8	C1, C2,
	T4	SR1, SR2, SR3, SR4, SR5, SR6	C1, C2, C3, C5, C4, C6
	T5	SR7	C7, C8
	T6	SR1, SR8	C1, C2, C5, C7
Приложения и базы данных	T7	SR9	C9, C18
	T8	SR10	C10, C11, C18
	T9	SR10, SR11	C10, C11, C18, C15
	T10	SR12	C12, C13
	T11	SR13	C14, C16, C17
	T12, T13	SR10, SR13	C10, C11, C18, C14, C16, C17
Сеть	T14	SR15, SR16	C19, C21, C22, C20
	T15	SR17, SR19	C16, C23, C24, C26
	T16, T17	SR16, SR19	C20, C26
	T18, T19	SR17, SR18	C16, C23, C24, C25
	T20	SR17, SR18, SR19	C16, C23, C24, C25, C26
Мобильные устройства	T21	SR20, SR22	C27, C29, C27
	T22	SR21, SR22	C28, C27, C29
	T23	SR22, SR23	C27, C29, C30

В соответствии с табл. 4 можно проводить следующие действия. Например, если необходимо устранить риск осуществления угрозы T7 «SQL-инъекции в систему информирования клиентов, SCADA-систему, платежную систему», то система должна удовлетворять требованию SR9 «Вводимые данные, используемые в SQL-запросах к системе информирования клиентов, SCADA-системе, платежной системе, должны тщательно проверяться», соответственно должны быть применены контрмеры C9 «Использовать фильтрацию входных данных в системе информирования клиентов, SCADA-системе, платежной системе», C18 «Использовать параметризированные запросы при обращении к базам данных системы информирования клиентов, SCADA-системы, платежной системы». Таким образом, данные табл. 4 позволяют определить, какие контрмеры должны быть применены при противодействии рассмотренным угрозам информационной безопасности, т.е. данную таблицу можно использовать в качестве базы правил при построении системы защиты.

Заключение. 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.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Концепция энергетической стратегии России на период до 2030 года (проект) // Энергетическая политика. – М.: ГУ ИЭС, 2007. Прил. – 116 с.
2. *Janssen M.C.* The Smart Grid Drivers // PAC World. – 2010. – 77 p.
3. *Amin S.M., Wollenberg B.F.* Toward a Smart Grid // IEEE P&E Magazine. – 2005. – № 3. – P. 34-41.
4. *Толшаков А.В.* SMART GRID: развитие, практика, проблемы // Энергонадзор. – 2014. – № 1. – URL: http://www.energosber18.ru/ru/propaganda/47-aespublications/613-smart-grid-development-practice-problems.html (дата обращения 20.12.2014).
5. *Гуревич В.И.* Интеллектуальные сети: новые перспективы или новые проблемы? // Электротехнический рынок. – 2010. – № 6. – URL: http://market.elec.ru/nomer/33/intellektualnye-seti-novye-perspektivy/ (дата обращения 15.07.2014).
6. *Smart Grid*. ENERGY.GOV Office of Electricity Delivery & Energy Reliability. – URL: http://www.oe.energy.gov/smartgrid.htm **(**дата обращения 15.07.2014).
7. *Шершень П.П., Ануфриев В.Н., Романов Д.Н.* В Витебске строят интеллектуальную сеть // Газ России. – 2010. – № 2. – С. 22-24.
8. *Дорофеев В.В., Макаров А.А.* Активно-адаптивная сеть – новое качество ЕЭС России // Энергоэксперт. – 2009. – № 4. – С. 28-34.
9. *Гарбук С.В.* Интеллектуальная система обеспечения информационной безопасности АСУ ТП КВО // Информационная безопасность. – 2015.
10. *Gruber T.* Toward Principles for the Design of Ontologies Used for Knowledge Sharing // International Journal Human-Computer Studies – Elsevier, 1995.
11. *Massel L.V.* Problems of the smart grid creation in Russia with a view to information and telecommunication technologies and proposed solutions // Proc. of the 15th International workshop “Computer science and information technologies” (CSIT’2013). Wien-Budapest-Bratislava, USATU. – 2013. – Vol. 1. – P. 115-120.
12. *Гаврилова Т.А.* Онтологический подход к управлению знаниями при разработке корпоративных систем автоматизации // Технологии менеджмента знаний центр компетенции по технологиям менеджмента на основе знаний. – 2010. – URL: http://kmtec.ru/ publications/library/authors/ontol_podhod_to_uz.shtml (дата обращения 20.12.2014).
13. *Arpirez J., Gomez- Perez A., Lozano A., Pinto S.* (ONTO) 2Agent: An ontology- based WWW broker to select Ontologies // Workshop on Applications of ontologies and Problem Solving Methods. ECAI. – 1998.
14. *Ворожцова Т.Н.* Разработка онтологии кибербезопасности в энергетике // Кибербезопасность-2013 // Материалы Международной научно-практической конференции. – Ялта, 2013.
15. *Mellado D., Fernández-Medina E., Piattini M.* Applying a Security Requirements Engineering Process // Proc. Security in Information Systems. – 2006. – P. 192-206.
16. Lund [and others]. Model-Driven Risk Analysis. – Milan: Springer, 2011. – 460 p.
17. *Муромцев Д.И.* Онтологический инжиниринг знаний в системе PROTÉGÉ: Методическое пособие. – СПб.: СПб ГУ ИТМО, 2007. – 62 с.
18. ГОСТ Р ИСО/МЭК 27001-2006**.** Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. – 32 с.
19. ГОСТ Р ИСО/МЭК 27005-2010**.** Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Требования. – М.: Стандартинформ, 2011. – 51 с.

20. *Пащенко И.Н., Васильев В.И.* Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 117-126.

REFERENCES

1. Kontseptsiya energeticheskoy strategii Rossii na period do 2030 goda (proekt) [The concept of the energy strategy of Russia for the period up to 2030 (draft)], *Energeticheskaya politika* [Energy Policy]. Moscow: GU IES, 2007. Pril., 116 p.
2. *Janssen M.C.* The Smart Grid Drivers, *PAC World*, 2010, 77 p.
3. *Amin S.M., Wollenberg B.F.* Toward a Smart Grid, *IEEE P&E Magazine*, 2005, No. 3, pp. 34-41.
4. *Tolshakov A.V.* SMART GRID: razvitie, praktika, problemy [SMART GRID: development, practice, problems], *Energonadzor* [Energonadzor], 2014, No. 1. Available at: http://www.energosber18.ru/ru/propaganda/47-aespublications/613-smart-grid-development-practice-problems.html (Accessed 20 December 2014).
5. *Gurevich V.I.* Intellektual'nye seti: novye perspektivy ili novye problemy? [Smart grid: new prospects or new problems?], *Elektrotekhnicheskiy rynok* [Electrical Market], 2010, No. 6. Available at: http://market.elec.ru/nomer/33/intellektualnye-seti-novye-perspektivy/ (Accessed 15 July 2014).
6. *Smart Grid*. ENERGY.GOV Office of Electricity Delivery & Energy Reliability. Available at: http://www.oe.energy.gov/smartgrid.htm **(**Accessed 15 July 2014).
7. *Shershen' P.P., Anufriev V.N., Romanov D.N.* V Vitebske stroyat intellektual'nuyu set' [In Vitebsk build intelligent network], *Gaz Rossii* [Gas Russia], 2010, No. 2, pp. 22-24.
8. *Dorofeev V.V., Makarov A.A.* Aktivno-adaptivnaya set' – novoe kachestvo EES Rossii [Active-adaptive network – a new quality of UES of Russia], *Energoekspert* [Energoekspert], 2009, No. 4, pp. 28-34.
9. *Garbuk S.V.* Intellektual'naya sistema obespecheniya informatsionnoy bezopasnosti ASU TP KVO [Intelligent system for information security APCS QUO], *Informatsionnaya bezopasnost' ASU TP KVO* [Information security APCS QUO], 2015.
10. *Gruber T.* Toward Principles for the Design of Ontologies Used for Knowledge Sharing, *International Journal Human-Computer Studies – Elsevier*, 1995.
11. *Massel L.V.* Problems of the smart grid creation in Russia with a view to information and telecommunication technologies and proposed solutions, *Proc. of the 15th International workshop "Computer science and information technologies" (CSIT'2013). Wien-Budapest-Bratislava, USATU*, 2013, Vol. 1, pp. 115-120.
12. *Gavrilova T.A.* Ontologicheskiy podkhod k upravleniyu znaniyami pri razrabotke korpo-rativnykh sistem avtomatizatsii [The ontological approach to knowledge management in the development of enterprise systems automation], *Tekhnologii menedzhmenta znaniy tsentr kompetentsii po tekhnologiyam menedzhmenta na osnove znaniy* [Technology knowledge management competence center technology management based on knowledge], 2010. Available at: http://kmtec.ru/ publications/library/authors/ontol_podhod_to_uz.shtml (Accessed 20 December 2014).
13. *Arpirez J., Gomez- Perez A., Lozano A., Pinto S.* (ONTO) 2Agent: An ontology- based WWW broker to select Ontologies, *Workshop on Applications of ontologies and Problem Solving Methods. ECAI*, 1998.
14. *Vorozhtsova T.N.* Razrabotka ontologii kiberbezopasnosti v energetike [The development of the ontology of cybersecurity in the energy sector], *Kiberbezopasnost'-2013: Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Materials of the International scientifically-practical conference]. Yalta, 2013.
15. *Mellado D., Fernández-Medina E., Piattini M.* Applying a Security Requirements Engineering Process, *Proc. Security in Information Systems*, 2006, pp. 192-206.
16. Lund [and others]. Model-Driven Risk Analysis. Milan: Springer, 2011, 460 p.
17. *Muromtsev D.I.* Ontologicheskiy inzhiniring znaniy v sisteme PROTÉGÉ: Metodicheskoe posobie [Ontological engineering knowledge in the PROTÉGÉ system: Toolkit]. St. Petersburg: SPb GU ITMO, 2007, 62 p.
18. *GOST R ISO/MEK 27001-2006.* Informatsionnaya tekhnologiya. Metody i sredstva obes-pecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya [State Standard R ISO/MEK 27001-2006. Information technology. Methods and means of security. Management system of information security. Requirements]. Moscow: Standartinform, 2008, 32 p.

19. *GOST R ISO/MEK 27005-2010*. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti. Trebovaniya [State Standard R ISO/MEK 27005-2010. Information technology. Methods and means of security. Risk management of information security. Requirements]. Moscow: Standartinform, 2011, 51 p.
20. *Pashchenko I.N., Vasil'ev V.I.* Razrabotka trebovaniy k sisteme zashchity informatsii v intellektual'noy seti Smart Grid na osnove standartov ISO/IEC 27001 i 27005 [Design of requirements to smart grid security system on the basis of ISO/IEC 27001 and 27005 standards], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 117-126.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Пащенко Иван Николаевич – Уфимский государственный авиационный технический университет; e-mail: iv.pashchenko@gmail.com; 450000, Уфа, ул. К. Маркса, 70; тел.: +73472730672; кафедра вычислительной техники и защиты информации; аспирант.

Васильев Владимир Иванович – e-mail: vasilyev@ugatu.ac.ru; кафедра вычислительной техники и защиты информации; зав. кафедрой; д.т.н.; профессор.

Гузаиров Мурат Бакеевич – e-mail: guzairov@rb.ru; кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

Pashchenko Ivan Nikolaevich – Ufa State Aviation Technical University; e-mail: iv.pashchenko@gmail.com; 12, K. Marxa street, Ufa, 450000, Russia; phone: +73472730672; the department of computer science and information security; postgraduate student.

Vasyliev Vladimir Ivanovich – e-mail: vasilyev@ugatu.ac.ru; the department of computer science and information security; head of department; dr. of eng. sc.; professor.

Guzairov Murat Bakeevich – e-mail: guzairov@rb.ru; the department of computer science and information security; dr. of eng. sc.; professor.

УДК 004.771

Е.Н. Тищенко, К.А. Буцик, В.В. Деревяшко

МОДЕЛЬ ДОВЕРЕННОЙ СЕТЕВОЙ ЗАГРУЗКИ «ТОНКОГО КЛИЕНТА» С НЕЙТРАЛИЗАЦИЕЙ «ВНУТРЕННЕГО НАРУШИТЕЛЯ»

Описана концепция и модель организации доверенной сетевой загрузки образа операционной системы в память рабочих станций, препятствующей атакам внутреннего нарушителя. Модель актуальна для существующих автоматизированных систем клиент-серверной архитектуры с терминальным доступом, построенных по технологии тонкий клиент (сетевая загрузка PXE и линии связи 100/1000Base-TX). Приводятся результаты анализа традиционных моделей и методов организации доверенной загрузки и возможностей внутреннего нарушителя по их обходу. Под традиционными моделями понимается использование специализированных программных и аппаратно-программных модулей доверенной загрузки, а также модифицированного программного обеспечения BIOS (UEFI). Для каждого метода (модели) приводятся актуальные направления (векторы) атак внутреннего нарушителя, что определяет недостатки использования метода. По результатам анализа предлагается концепция и технологическая реализация новой модели доверенной сетевой загрузки, лишенная выявленных недостатков. В базисе новой модели лежит контроль временных интервалов штатного обмена запросами на загрузку операционной системы между рабочей станцией и сервером. Новая модель основана на использовании периферийных сетевых модулей и центрального контроллера совместно с рабочими станциями и серверным массивом соответственно, что позволяет управлять состоянием межсетевого экрана и сервера сетевой загрузки в режиме реального времени и обеспечивает мгновенную блокировку прохождения сетевого трафика к защищаемым узлам автоматизиро-