4. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 2 (22).– С. 257-259.
5. *Миронова В.Г., Шелупанов А.А.* Модель нарушителя безопасности конфиденциальной информации // Информатика и системы управления. – 2012. – № 1 (31). – С. 28-35.
6. *Миронова В.Г., Шелупанов А.А.* Сети Петри как инструмент анализа системы защиты конфиденциальной информации // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 64-70.
7. *Миронова В.Г., Шелупанов А.А*. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 2 (22). – С. 257-259.
8. *Шелупанов А.А., Миронова В.Г. и др.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Ч. 1. – 2010. – № 1 (21). – С. 14-22.

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Миронова Валентина Григорьевна – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники»; e-mail: mvg@security.tomsk.ru; 634050, г. Томск, пр. Ленина, 40; тел.: 89234151608; руководитель аттестационного цента института системной интеграции и безопасности ТУСУРа.

Шелупанов Александр Александрович – e-mail: saa@udcs.ru; тел.: +73822514302; д.т.н.; профессор; проректор по научной работе ТУСУРа.

Mironova Valentina Grigor'evna – Tomsk State University of Control Systems and Radio Electronics; e-mail: mvg@security.tomsk.ru; 40, Lenin avenue, Tomsk, 634050, Russia; phone: +79234151608; the head of the appraisal institute cents systems integration and security TUSUR.

Shelupanov Alexander Alexandrovich – e-mail: saa@udcs.ru; phone: +73822514302; dr. of eng. sc.; professor; vice-rector TUSUR.

УДК 004.735

И.Н. Пащенко, В.И. Васильев

РАЗРАБОТКА ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНОЙ СЕТИ SMART GRID НА ОСНОВЕ СТАНДАРТОВ ISO/IEC 27001 И 27005

Приоритетным направлением развития современной энергетики Российской Федерации является внедрение интеллектуальных энергосетей нового поколения Smart Grid. Однако как в отечественной, так и в зарубежной литературе не уделяется достаточного внимания вопросам защиты информации в подобных интеллектуальных сетях. Целью данной работы является разработка методики создания системы защиты информации в Smart Grid сетях с учетом того, что данные сети пока еще не внедрены, а их внедрение займет определенный промежуток времени. Приводится список основных угроз и уязвимостей информационной безопасности, которым подвержены Smart Grid сети. Предлагается список руководящих требований безопасности, которые необходимо выполнить при проектировании данных интеллектуальных сетей. Формируется список контрмер, которые рекомендуются для применения на Smart Grid. Рассчитывается эффективность применения контрмер путем оценки рисков информационной безопасности до и после их внедрения на примере конкретной Smart Grid сети.

Интеллектуальная сеть угрозы; уязвимости; информационные риски.

I.N. Pashchenko, V.I. Vasilyev

DESIGN OF REQUIREMENTS TO SMART GRID SECURITY SYSTEM ON THE BASIS OF ISO/IEC 27001 AND 27005 STANDARDS

The important stage in development of modern energy technology is implementing intelligent energy nets of new generation Smart Grid. The purpose of this work is to design the technique of creating the information security system in intelligent nets (Smart Grid) with account of that the given nets are not yet implemented, and their implementation needs some time interval. The list of main threats and vulnerabilities in Smart Grid is presented. The list of guiding security requirements necessary under designing these nets is proposed. The list of security controls recommended for using in Smart Grid is generated. The efficiency of applying countermeasures by the way of information security risks evaluation before and after their implementation on the specific Smart Grid is calculated.

Intelligent net; Smart Grid; threats; vulnerabilities; information risks.

Согласно “Энергетической стратегии России на период до 2030 г. ”[1], в качестве первого пункта стратегии развития энергетики указывается создание в России интеллектуальных сетей Smart Grid.

Под интеллектуальной сетью (Smart Grid) 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.

Первые применения этого термина на Западе были связаны с названиями специальных контроллеров, предназначенных для управления режимом работы и синхронизации автономных ветрогенераторов, отличающихся нестабильным напряжением и частотой, с электрической сетью [2, 3]. Потом этот термин стал применяться для обозначения микропроцессорных счетчиков электроэнергии, способных самостоятельно накапливать, обрабатывать, оценивать информацию и передавать ее по специальным каналам связи и даже через Интернет. В последние годы использование этого термина расширилось на системы сбора и обработки информации, мониторинга оборудования в энергетике [4].

С точки зрения Министерства энергетики США, интеллектуальным сетям (Smart Grid) присущи следующие атрибуты [5]:

- способность к самовосстановлению после сбоев в подаче электроэнергии;
- возможность активного участия потребителей;
- устойчивость к физическому и кибернетическому вмешательству злоумышленников;
- обеспечение требуемого качества передаваемой электроэнергии;
- обеспечение синхронной работы источников генерации и узлов хранения электроэнергии;
- повышение эффективности работы энергосистемы в целом.

В России идея Smart Grid в настоящее время выступает в качестве концепции интеллектуальной активно-адаптивной сети, которую можно описать следующими признаками [6]:

- насыщенность сети активными элементами, позволяющими изменять топологические параметры сети;
- большое количество датчиков, измеряющих текущие режимные параметры для оценки состояния сети в различных режимах работы энергосистемы;
- наличие системы сбора и обработки данных (программно-аппаратные комплексы), а также средств управления активными элементами сети и электроустановками потребителей;

- наличие исполнительных механизмов, позволяющих в режиме реального времени изменять топологические параметры сети, а также взаимодействовать со смежными энергетическими объектами;
- использование средств автоматической оценки текущей ситуации и прогнозирования работы сети;
- высокая производительность системы управления сетью в целом и системы информационного обмена.

В настоящее время в России много внимания уделяется различным пилотным проектам, направленным на создание сетей Smart Grid [7]. Проводятся конференции, на которых обсуждаются проблемы создания и внедрения подобных сетей нового поколения. Примером таких конференций является SmartUtilities Russia 2013.

Одной из актуальных проблем в области создания интеллектуальных сетей является проблема обеспечения их информационной безопасности. В данной работе предлагается проект разработки системы защиты информации для сети Smart Grid.

В настоящее время в России не существует окончательно сформированной работающей интеллектуальной сети, удовлетворяющей всем требованиям, предъявляемым к Smart Grid. Большинство сетей в настоящее время находятся на стадии проектирования. Поэтому разрабатываемые ниже требования к системе защиты информации направлены в первую очередь на построение перспективных Smart Grid сетей, которые предполагаются к использованию в ближайшем будущем. Внедрение подобных интеллектуальных сетей требует определенного времени. В течение этого времени появятся новые средства защиты информации, которые необходимо будет установить на Smart Grid.

С целью разработки системы защиты Smart Grid было принято решение произвести оценку рисков информационной безопасности с учетом следующих основных аспектов:

- *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 и CORAS, разработанных в соответствии с международным стандартом ISO/IEC 27001 [8].

SREP (Security Requirements Engineering Process) – метод, целью которого является разработка требований к системе защиты информации [9]. Он состоит из девяти шагов:

1. Введение основных определений.
2. Выбор критических/уязвимых источников информации.
3. Постановка целей для системы защиты информации.
4. Определение угроз.
5. Определение рисков.
6. Разработка требований к системе защиты.
7. Упорядочивание требований по важности.
8. Проверка соответствия существующей системы разработанным требованиям.
9. Разработка контрмер.

CORAS – метод проведения анализа информационных рисков [10]. Он состоит из восьми шагов:

1. Подготовка к проведению анализа.
2. Выбор объектов защиты.
3. Описание объектов защиты с помощью диаграмм.
4. Постановка целей.
5. Идентификация рисков с помощью диаграмм Угроз.
6. Определение рисков по диаграммам Угроз.
7. Оценка риска с использованием диаграмм Рисков.
8. Разработка контрмер с использованием диаграмм Контрмер.

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

Оценка возможного риска происходила в соответствии с методологией, предложенной в стандарте ISO/IEC 27005 [11].

В результате анализа были выделены три вида информационных ресурсов, подлежащих защите:

1. Персональные данные пользователей Smart Grid.
2. Техническая информация, поступающая от клиентов сети.
3. 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 (конфиденциальность);
- обеспечение постоянного доступа пользователей к защищаемой информации (доступность);
- предотвращение несанкционированного изменения защищаемой информации (целостность).

В результате исследования были выделены основные угрозы безопасности Smart Grid, представленные в табл. 1.

Таблица 1

Угрозы безопасности Smart Grid

№	Угрозы
	Менеджмент
1	Неавторизованное раскрытие/изменение/лишение доступа к персональным данным/техническим данным/данным об отказах в результате неверного распределения прав доступа к системам Smart Grid
2	Неавторизованное раскрытие/изменение/лишение доступа к персональным данным в результате сбоя/не произведения обновления систем, функционирующих в Smart Grid
3	Неавторизованное изменение/лишение доступа к техническим данным/ данным об отказах в результате сбоя/не произведения обновления систем, функционирующих в Smart Grid
4	Неавторизованное раскрытие персональных данных в результате небрежного отношения работников к своим обязанностям
5	Неавторизованное изменение/лишение доступа к персональным данным/техническим данным/данным об отказах в результате закупки либо установки ненужных систем безопасности
6	Неавторизованное раскрытие/изменение/лишение доступа к персональным данным/техническим данным/данным об отказах в результате беспечности либо некомпетентности администратора систем SCADA

Окончание табл. 1

Приложения и базы данных	
7	SQL-инъекции в систему информирования клиентов, SCADA систему, платежную систему
8	XSS атаки на систему информирования клиентов
9	Атаки на неавторизованную аутентификацию в системе информирования клиентов
10	Атаки на SSL
11	Backdoor'ы, трояны и др. вредоносные программы
12	Подбор пароля методом «грубой силы»
13	DDoS атака на систему информирования клиентов/SCADA систему
Сеть	
14	Перехват пакетов системы информирования клиентов
15	Сканирование портов
16	Подмена IP-адресов системы информирования клиентов/SCADA системы
17	Кража TCP-пакетов системы информирования клиентов
18	Атака типа отказ в обслуживании системы информирования клиентов/SCADA системы
19	TCP SYN-атака на систему информирования клиентов
20	Смурф-атака на систему информирования клиентов/SCADA систему
Мобильные устройства	
21	Неавторизованное раскрытие/изменение персональных данных/ технических данных/данных об отказах в результате извлечения информации из утерянного/украденного устройства
22	Неавторизованное раскрытие/изменение персональных данных/ технических данных/данных об отказах в результате использования списанного/неверно обновленного устройства
23	Неавторизованное раскрытие/изменение персональных данных/ технических данных/данных об отказах в результате сбоя/не произведения обновления мобильного устройства

Для устранения указанных угроз были выделены требования по безопасности Smart Grid. Перечень основных требований к системе информационной безопасности Smart Grid представлен в табл. 2.

Таблица 2

Требования к безопасности

№	Требование
Менеджмент	
1	Должна быть задокументирована персональная ответственность за выполнение всех действий всеми пользователями Smart Grid
2	Должны быть четко указаны роли пользователей Smart Grid
3	Должны быть указаны алгоритмы автоматического присвоения ролей для новых пользователей Smart Grid
4	Должны быть указаны действия, разрешенные для каждой роли
5	Должно быть указано, что разрешается/запрещается делать по умолчанию для всех пользователей Smart Grid
6	Должны быть указаны процедуры при прекращении срока действия роли
7	Должно быть обеспечено эффективное инвестирование в системы безопасности Smart Grid
8	Процесс поиска и оценки угроз должен проводиться регулярно
Приложения и базы данных	
9	Вводимые данные, используемые в SQL-запросах к системе информирования клиентов/SCADA/платежной системе, должны тщательно проверяться
10	Вводимые данные на сайте системы информирования клиентов должны тщательно проверяться

Окончание табл. 2

11	В системе информирования клиентов должны использоваться протестированные методы аутентификации, основанные на собственном способе аутентификации клиентов
12	Все мандаты доступа к системе информирования клиентов должны храниться в хешированном виде
13	Должна использоваться эффективная система защиты Smart Grid от вредоносного ПО
14	Должна быть обеспечена доступность системы информирования клиентов и SCADA системы
Сеть	
15	Содержание передаваемых пакетов должно защищаться и верифицироваться
16	Должны быть разработаны мандатные управленческие функции для системы информирования клиентов/SCADA системы
17	Должно использоваться только проверенное и эффективное ПО
18	Должны применяться методы аутентификации при доступе к DNS-серверу
19	Должно использоваться защищенное TCP соединение
Мобильные устройства	
20	Должно быть обеспечено безопасное удаление важной информации
21	Должны быть разработаны действия, которые необходимо применять в случае списания устройства
22	Должна быть разработана система защиты информации от несанкционированного раскрытия и модификации важной информации
23	ПО должно своевременно обновляться

Для того чтобы снизить вероятность реализации угроз злоумышленниками до приемлемого уровня, были предложены соответствующие контрмеры. Список основных контрмер представлен в табл. 3.

Таблица 3

Контрмеры

№	Контрмера
Менеджмент	
1	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
2	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
3	Политика доступа к системе Smart Grid должна быть разработана, задокументирована и пересмотрена, основываясь на требованиях, предъявляемых бизнесом и безопасностью
4	Должны быть разработаны механизмы регистрации и дерегистрации пользователей (клиентов, менеджеров, администраторов SCADA, администраторов Smart Grid) во всех точках входа в систему Smart Grid
5	Служба безопасности Smart Grid должна регулярно пересматривать права доступа пользователей Smart Grid через установленные промежутки времени
6	Права доступа всех работников должны удаляться после истечения их срока контракта либо изменяться при его обновлении
7	Должен быть разработан шаблон оценки угроз. Переоценка угроз должна осуществляться каждые 6 месяцев
8	В соответствии с экономическим анализом системы информационной безопасности должен быть составлен экономически обоснованный отчет, который впоследствии должен быть использован при выборе необходимых улучшений в системе информационной безопасности

Окончание табл. 3

Приложения и базы данных	
9	Использовать фильтрацию входных данных в системе информирования клиентов/SCADA системе/платежной системе
10	Использовать межсетевой экран веб-приложений для сайта системы информирования клиентов
11	Использовать криптографические токены для аутентификации работников
12	Использовать SSL с сертификатами
13	Использовать SSL везде, где доступ требует аутентификации пользователя
14	Использовать ПО, позволяющее проводить тестирование безопасности веб-приложений, такое как WebScarab
15	Ограничить число попыток ввода пароля пользователям при входе в систему информирования клиента/SCADA систему
16	Использовать ПО, позволяющее противостоять вирусам, вредоносному ПО, а также использовать межсетевые экраны
17	Использовать оборудование, позволяющее отражать атаки типа отказ в обслуживании, например DefensePro
18	Использовать параметризированные запросы при обращении к базам данных системы информирования клиентов/SCADA системы/платежной системы
Сеть	
19	Использовать шифрование при формировании и передаче пакетов
20	Использовать межсетевой экран для серверов системы информирования клиентов/SCADA системы
21	Использовать системы обнаружения вторжения (NIDS) для Smart Grid
22	Использовать прокси-сервер
23	Периодически сканировать сетевые порты, чтобы обнаружить незащищенные порты
24	Использовать обновленное ПО
25	Использовать систему авторизации для доступа к DNS-серверу
26	Использовать фильтрацию пакетов
Мобильные устройства	
27	Использовать политику информационной безопасности Google Apps Device Policy
28	Разработать корпоративную политику списания мобильных устройств
29	Использовать мобильные антивирусы
30	Проводить регулярное обновление мобильных устройств

После формирования контрмер для конкретной сети были оценены риски информационной безопасности до и после введения контрмер. Данные оценки рисков представлены в табл. 4–7.

Таблица 4

Изменение риска на уровне Менеджмента

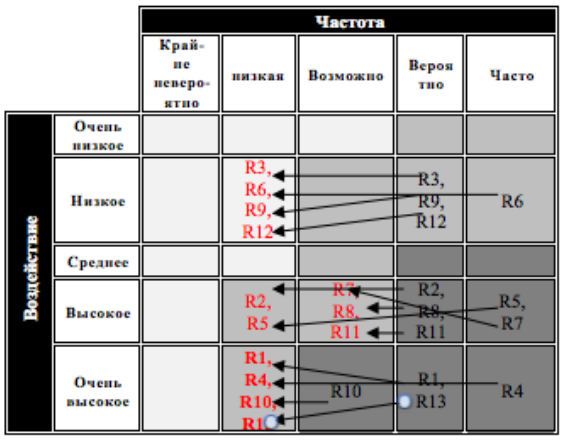


Таблица 5

Изменение риска на уровне Приложений и баз данных

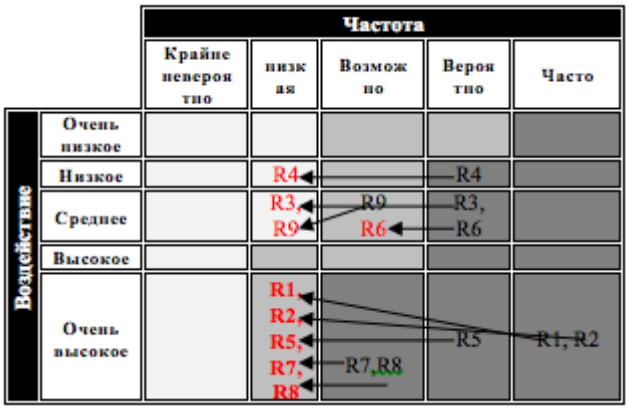


Таблица 6

Изменение риска на уровне Сети

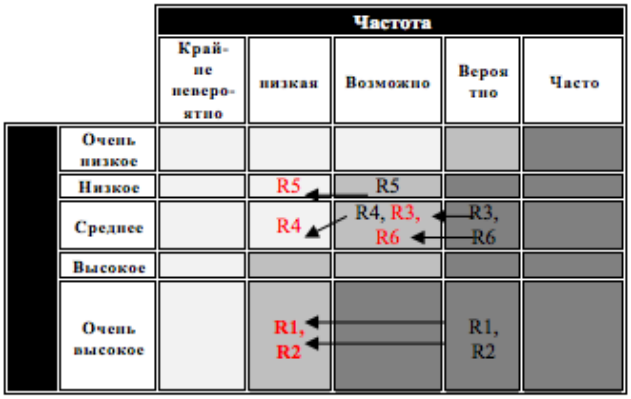
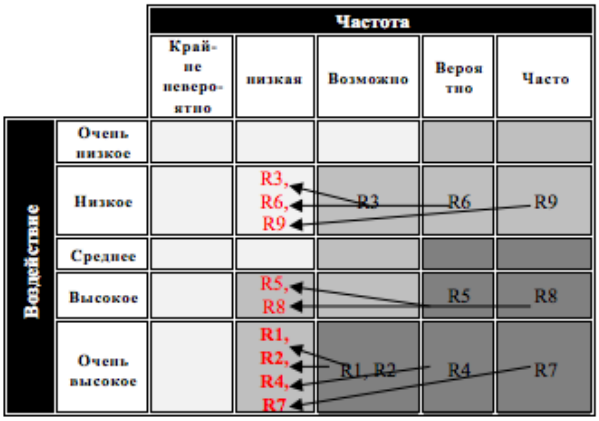


Таблица 7

Изменение риска на уровне Мобильных устройств



Все риски были разделены на высокие, средние и низкие. Высокий уровень риска нарушения информационной безопасности означает, что данную угрозу необходимо устранять. Средний уровень риска говорит о том, что ситуация не является критической, однако нужно следить за развитием данных угроз. Низкий уровень риска является приемлемым для работы сети.

В результате анализа защищенности сети с использованием данных контрмер было выявлено, что учитываемые риски осуществления рассматриваемых уязвимостей становятся приемлемыми для работы сети. Таким образом, можно говорить о том, что проектируемая Smart Grid с использованием предложенных мер безопасности может считаться защищенной.

Заключение. Smart Grid представляют собой новый перспективный класс энергосетей. В наши дни происходит преобразование существующих энергосетей в соответствии с теми требованиями, которые возникают при модернизации этих сетей в сети класса Smart Grid. В настоящее время не существует формализованной методологии разработки систем защиты информации для подобных интеллектуальных сетей. В данной работе предложена методика анализа защищенности сетей Smart Grid, проведен анализ типовых угроз и уязвимостей, которым подвержена основная часть сети Utility, разработаны требования к системе информационной безопасности Smart Grid, предложены мероприятия по противодействию выявленным угрозам.

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. – P. 77.
3. *Amin S.M., Wollenberg B.F.* Toward a Smart Grid // IEEE P&E Magazine. – 2005. – № 3. – P. 34-41.
4. *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 15.07.2013).
5. Smart Grid // ENERGY.GOV Office of Electricity Delivery & Energy Reliability. URL: http://www.oe.energy.gov/smartgrid.htm (дата обращения 15.07.2013).
6. *Дорофеев В.В., Макаров А.А.* Активно-адаптивная сеть – новое качество ЕЭС России // Энергоэксперт. – 2009. – № 4. – С. 28-34.
7. *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). – 2013. – P. 115-120.
8. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin : ISO/IEC JTC 1/SC 27. – 2013. – 23 p.
9. *Mellado D., Fernández-Medina E., Piattini M.* Applying a Security Requirements Engineering Process // Proc. Security in Information Systems. – 2006. – P. 192-206.
10. Model-Driven Risk Analysis / Lund [and others]. Milan: Springer, 2011. – 460 p.
11. ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management. Berlin : ISO/IEC JTC 1/SC 27, 2011. – 68 p.

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

Пащенко Иван Николаевич – Уфимский государственный авиационный технический университет; e-mail: iv.pashchenko@gmail.com; 450000, г. 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.

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 the department; dr. of eng. sc.; professor.

УДК 004.056

И.Ю. Половко

РАЗРАБОТКА ТРЕБОВАНИЙ К СОСТАВУ ХАРАКТЕРИСТИК ДЛЯ СРАВНЕНИЯ СОА*

Работа посвящена актуальной проблеме выбора средства защиты, для обеспечения надежной работы компьютерной сети. В качестве средства защиты рассматривается система обнаружения атак (СОА). Обоснована необходимость выработки требований к составу качественных характеристик СОА, позволяющих получить взвешенную оценку качества исследуемых систем.

Показано, что характеристики структурно делятся на две группы – для оценки функциональных свойств системы и для оценки производительности. Обоснован выбор данных характеристик. При разработке характеристик оценки качества СОА исследовались, в первую очередь, те механизмы СОА, которые наиболее критичны для атак, а значит, могут повлиять на эффективность обнаружения атак. Выявлены наиболее уязвимые аспекты в работе СОА при обнаружении атак. Для этого был рассмотрен подход, основанный на исследовании слабых сторон протоколов, использование которых позволяет легально обойти механизмы СОА. Таким образом, показано, что СОА, чётко следующие RFC, оказываются уязвимыми. Разработанные характеристики позволяют оценить степени соответствия реальных и заявленных производителем функциональных свойств СОА.

Сетевая безопасность; СОА; характеристики качества; критерии оценки.

I.Yu. Polovko

THE DEVELOPMENT OF REQUIREMENTS TO THE CHARACTERISTICS OF NIDS FOR COMPARISON

The scientific work is devoted to the actual problem of selecting protection to provide reliable operation of the network. As a means of protection consider the intrusion detection system (NIDS). The necessity of developing requirements to the structure of quality characteristics of NIDS, was justified. That allowing to obtain a balanced quality assessment of the systems.

The characteristics structurally divided into two groups – to evaluate the functional properties of the system and for performance evaluation. The choice of, these characteristics was justified. Primarily was investigated mechanisms of NIDS, during the development of characteristics of the NIDS, that are most critical for the attack, thus may affect on efficiency of detection of attacks. Has been identified the most vulnerable aspects of NIDS at the detection of attacks. For this was considered an approach based on a study of the weaknesses of protocols, the using of which allows you to legally circumvent the mechanisms of NIDS. That is shown that the NIDS that are clearly following RFC, are vulnerable. The developed characteristics allows to estimate the compliance of the real and the manufacturer's functional properties of NIDS.

Network security; NIDS; quality characteristics; evaluation criteria.

* Работа выполнена при поддержке гранта РФФИ № 12-07-00014-а.