Meshcheriakov Roman Valerievich – e-mail: mrv@security.tomsk.ru; phone +73822413426; dr. of eng. sc.; professor.

Hodashinsky Ilya Alexandrovich – e-mail: hodashn@rambler.ru; phone/fax: +73822900111; dr. of eng. sc.; professor.

УДК 004.056

М.Н. Жукова, Н.А. Коромыслов

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ*

Рассматривается подход к построению защищенных автоматизированных систем. Проанализированы существующие решения в области анализа защищенности, показаны трудности их применения на территории РФ. Предложен и описан подход, основанный на применении аппарата нечеткой логики. Представлена модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики. Описаны основные составляющие модели и процедура интеграции статистических данных, накопленных автоматизированной системой в процессе функционирования. Предложено применение прецедентного подхода к разработке модифицированного алгоритма оценки защищенности автоматизированной системы. За счет применения механизмов нечеткой логики отсутствуют требования к строгой формализации данных и появляется возможность работы с качественными характеристиками. Однако остается проблемы предварительной настройки некоторых параметров, таких как, выбор представления лингвистических переменных; определение граничных значений термов; выбор метода дефаззификации. На основе предложенной модели разработан алгоритм автоматизированной системы на прецедентах оценки защищенности АС, представлена его схема. Таким образом, проведено объединение трех подходов к оценке и анализу защищенности АС: использование стандартизированного подхода; использование результатов работы СЗИ АС; использование аппарата нечеткой логики. Эффективное сочетание данных подходов позволяет, предусмотреть требования стандартов, учесть прецеденты ИБ, что позволит более динамично управлять АС и с большей эффективностью оценивать защищенность.

Информационная безопасность; автоматизированная система; оценка защищенности; нечеткая логика

M.N. Zhukova, N.A. Koromyslov

MODEL OF THE AUTOMATED SYSTEM SECURITY ASSESSMENT WITH USE OF THE FUZZY LOGIC

Approach to creation of the protected automated systems is considered. Existing decisions in the field of the security analysis are analysed, difficulties of their application in the territory of the Russian Federation are shown. The approach based on use of the fuzzy logic is offered and described. The model of an assessment of automated system security with use of the fuzzy logic is presented. The main components of model and procedure of statistical data integration which have been saved up by automated system in the course of functioning are described. Application of case approach to development of the modified algorithm of an assessment of the automated system security is offered. At the expense of use of the fuzzy logic mechanisms there are no requirements to strict formalization of data and there is a possibility to work with qualitative characteristics. However there are problems of preliminary control of some parameters, such as, a choice of linguistic variables representation; determination of boundary values of terms; choice of a

* Работа выполнена при финансовой поддержке РФФИ, соглашение НК 13-07-00222\13 от 09.04.2013 г.

defazzification's method. On the basis of the offered model the algorithm of the automated system on cases of the security assessment to information system security for automated systems is developed, his scheme is submitted. Thus, association of three approaches to an assessment and the security analysis is carried out: use of the standardized approach; use the results of work in information system security for automated systems; use of the fuzzy logic. The effective combination of these approaches allows, to provide requirements of standards, to consider cases that will allow to operate more dynamically and with bigger efficiency to estimate security.

Information security; automated system; assessment of security; fuzzy logic.

При построении системы защиты информации (СЗИ) сложился подход, основанный на представлении процесса обработки информации в виде абстрактной вычислительной среды, в которой работают множество «субъектов» (пользователей и процессов) с множеством «объектов» (ресурсы и наборы данных) [1]. При этом процесс построения СЗИ заключается в создании защитной среды в виде некоторого множества ограничений и процедур, способных под управлением ядра безопасности запретить несанкционированный и реализовать санкционированный доступ «субъектов» к «объектам» и защиту последних от множества преднамеренных и случайных внешних и внутренних угроз.

Данный подход опирается на теоретические модели безопасности: АДЕПТ-50 Хартсона, Белла–Лападулы, MMS Лендвера и МакЛина, Биба, Кларка–Вилсона и др [2]. Считается, что перечисленные модели являются инструментарием при разработке определенных политик безопасности, определяющих некоторое множество требований, которые должны быть выполнены в конкретной реализации системы. На практике разработчику чрезвычайно сложно реализовать эти модели, и поэтому они рекомендуются лишь для анализа и оценки «уровня безопасности» автоматизированных систем (АС), а руководствоваться предлагается специально разработанными на основе упомянутых подхода и моделей стандартами.

Существует достаточно большое количество нормативно-методических документов, определяющих требования к защищенным системам и порядок их создания [3, 4]. Вместе с тем, подавляющее большинство из них предлагают реализацию индивидуального проектирования СЗИ, выражающегося в построении автоматизированных систем в защищенном исполнении (АСЗИ) с использованием концепции нисходящего проектирования [1]. Несмотря на очевидные достоинства, такой подход требует значительных временных и материальных затрат. При этом, в последние несколько лет, наблюдается значительный рост объема рынка средств защиты информации (СрЗИ), что предопределило возможность реализации концепции восходящего проектирования с использованием типовых решений по средствам защиты, которая является более доступной для большинства негосударственных учреждений, не оперирующих информацией содержащей государственные секреты и обладающих невысоким бюджетом.

Очевидно, что одной из важнейших задач оптимального построения комплексной СЗИ является выбор из множества имеющихся средств такого их набора, который позволит обеспечить нейтрализацию всех потенциально возможных информационных угроз с наилучшим качеством и минимально возможными затраченными на это ресурсами [5]. При этом на многочисленных практических примерах, доказано, что наиболее эффективно задачи защиты информации решаются в рамках упреждающей стратегии защиты, когда на этапе проектирования оцениваются потенциально возможные угрозы и реализуются механизмы защиты от них [6]. Ключевым моментом в этой ситуации является также то, что, на этапе проектирования СЗИ, разработчик, не имея статистических данных о результатах функционирования создаваемой системы, вынужден принимать решение о составе комплекса СрЗИ, находясь в условиях значительной неопределенности [7].

Необходимость оперативного решения задачи моделирования и оптимизации архитектуры защищенной АС, определения ее параметров, поиск их оптимальных значений и т.д. привели к созданию нескольких направлений теоретических и практических исследований:

- работы, посвященные анализу защищенности автоматизированных систем;
- работы, посвященные исследованиям в области интегрированного управления информационными и другими типами рисков;
- работы, посвященные исследованиям в области анализа комплексных нарушений в системах защиты информации и анализа безопасности в условиях неполной информации и др.

Данные направления открывают возможности по созданию разнообразных программных решений, направленных на решение части задач, например:

- MaxPatrol, XSpider, Tenable Nessus, Appradar, AppDetectivePro – системы анализа защищенности;
- Dbprotect, SecureSphere DataBase Security Gateway, SecureSphere Database Monitoring Gateway, MaxPatrol – комплексные системы управления защищенностью;
- CiscoWorks Network Compliance Manager, IBM Ilog, JBoss Enterprise BRMS, Oracle Business Rules – аналитические системы поддержки принятия решений (анализ соответствия бизнес-модели, стандартам безопасности, политике безопасности и т.д.).

Данные системы играют ключевую роль при решении той или иной задачи, возникающей в процессе построения защищенной АС. Наиболее известными компаниями, занимающимися разработками флагманских систем данного класса являются IBM, Cisco, Positive Technologies, Symantec, Nessus, ФГУП «Концерн «СИСТЕМПРОМ»» и др. Для анализа и комплексной оценки защищенности АС компании, в своих решениях, применяют эксклюзивные алгоритмы собственного производства, которые для потребителей являются, по сути, «черным ящиком». Данный факт и стоимость предлагаемых решений делает их применение на территории РФ затруднительным. Это обусловлено в первую очередь тем, что для применения на АС, обрабатывающих конфиденциальную информацию на территории РФ, должны применяться решения удовлетворяющие требованиям регуляторов в сфере ИБ (ФСТЭК России, ФСБ России), т.е. пройти проверку на соответствие и иметь сертификат регулятора. Для прохождения проверки на соответствие компаниям необходимо предоставить регуляторам исходные коды программной реализации алгоритмического обеспечения своих решений, что не всегда является приемлемым по ряду причин. А использование не сертифицированных решений для организации защищенных АС на территории РФ является нелигитимным. Закрытость, стоимость, отсутствие сертификатов регуляторов практически не позволяют на территории РФ проектировать и внедрять защищенные АС, спроектированные и проанализированные на базе систем данного класса.

Однако именно алгоритмическое обеспечение систем подобного класса является инновационным продуктом и позволяет существенно повысить уровень разработки защищенных АС с предварительным моделированием и оптимизацией параметров, оценкой уровня защищенности, обеспечением заданного уровня надежности и прогнозированием уровня защищенности АС при различных изменениях жизненного цикла системы.

Выходом из сложившейся ситуации является разработка и(или) модификация алгоритмов анализа защищенности АС на базе уже существующих подходов с привлечением механизмов, которые позволят адаптировать алгоритмы к изменениям, происходящим в АС в процессе ее эксплуатации.

Основу алгоритмического обеспечения должны составлять интеллектуальные алгоритмы моделирования и оптимизации, анализа защищенности, а также алгоритмы оценки надежности и прогнозирования модифицированные с помощью современного математического аппарата. В рамках данного исследования предлагается применение аппарата нечеткой логики для модификации алгоритма анализа защищенности АС. Применение модификаций с помощью методов, относящихся к технологии «мягких вычислений», позволят модифицированным алгоритмам приобрести свойства, перспективные с точки зрения защиты информации: распознавание, разнообразие, обучение, самообучение, память, распределенный поиск, высокая скорость поиска оптимальных решений, внутренняя регуляция и адаптивность [8]. Их применение закономерно с точки зрения требований к АС в условиях постоянно изменяющихся состояний АС в течение жизненного цикла системы – уровень защищенности АС должен быть максимально стабильным и отвечающим заданным требованиям. Только такие АС имеют высокую вероятность противостоять новым, ранее неизвестным инцидентам ИБ.

Анализ защищенности АС невозможен без оценки на соответствие требованиям того или иного нормативного документа. Процедуру оценки, как правило, проводят с применением различных методов опроса. Основными этапами данного подхода (являются: использование опросных листов на основе требований стандарта; формирование базы знаний (на основе требований и рекомендаций стандарта, на основе мнений привлеченных специалистов – экспертов); нахождение правил по анализу ответов на опросные листы. Применение только стандартизированного (табличного) подхода позволит достаточно быстро построить оценку защищенности и получить рекомендации для АС. Но, к сожалению, реализация полученных рекомендаций практически всегда затруднена (или невозможна) из-за того, что не стандарт не учитывает информацию, накопленную самой системой в процессе ее функционирования.

Таким образом, возникает задача одновременного учета и требований стандарта и статистики (например, по инцидентам информационной безопасности), собранной в процессе функционирования АС. Однако, учет всех произошедших инцидентов невозможен в силу огромного разнообразия в видах событий и большого их числа, происходящих даже в небольшой АС в процессе ее функционирования. Таким образом, необходимо из огромного числа зафиксированных инцидентов сформировать базу прецедентов, с которой далее будет работать алгоритм анализа защищенности. Прецедент – случай, имевший место ранее и служащий примером или оправданием для последующих случаев подобного рода. База прецедентов формируется из базы инцидентов, сформированной, например, из log-файлов системы обнаружения вторжений/системы обнаружения атак. В принципе, для формирования базы прецедентов, можно использовать журналы межсетевых экранов и других средств защиты информации, а так же операционных систем и т.д.

В основе модифицированного алгоритма анализа защищенности лежит модель оценки защищенности, построенная с применением аппарата нечеткой логики [9], представленная на рис. 1.

Наибольший интерес в представленной модели представляют механизмы применения аппарата нечеткой логики. Для корректной работы данного блока необходима информация из базы прецедентов. База прецедентов формируется из базы инцидентов, зарегистрированных в АС. При этом, система весьма гибка, так как базу прецедентов можно формировать любым способом, исходя из особенностей назначения АС, требований к ее функционированию, требований к организации защиты информации и т.д. Это помогает в определении управляющих воздействий пользователя на тот или иной прецедент ИБ в соответствии с требованиями,

а так же определяет порядок реализации данных действий от наиболее критичных, в результате невыполнения которых имеется реальная возможность утечки (потери, искажения и т.д.) информации, до наименее критичных, в результате невыполнения которых создаются предпосылки для утечки информации.

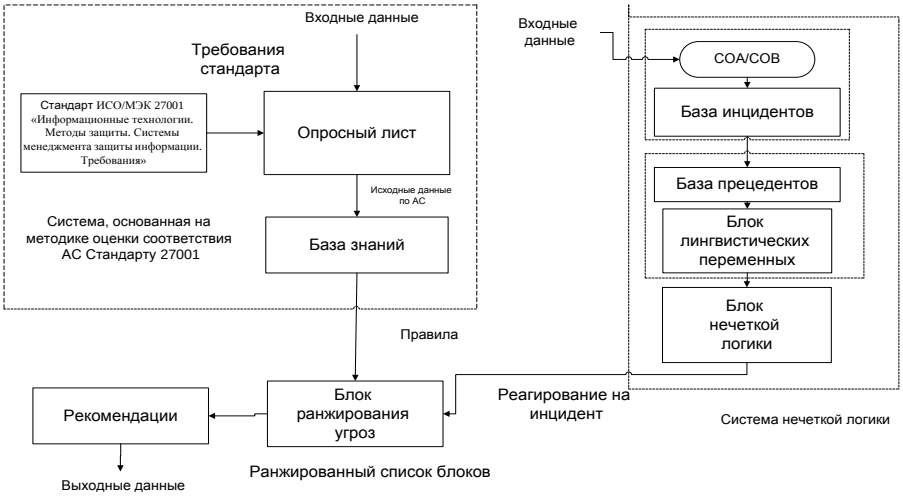

Рис. 1. Схема модели оценки защищенности АС с применением механизмов нечеткой логики

Таким образом, на вход блока «нечеткой логики» подаются те параметры, которые выбраны для оценки. Одной из особенностей применения механизмов нечеткой логики является отсутствие требований к строгой формализации данных и возможность работы с качественными характеристиками. Однако для корректной работы требуется предварительная настройка некоторых параметров, таких как:

- ♦ выбор представления лингвистических переменных;
- ♦ определение граничных значений термов;
- ♦ выбор методы дефаззификации.

Решение данной задачи, в свою очередь, требует достаточно высокой квалификации от пользователя. Вся остальная процедура обработки представлена для пользователя в виде «черного ящика» – на вход системы с нечеткой логикой подаются параметры, выбранные для оценивания, на выходе формируется определенное управляющее воздействие. Управляющие воздействия поступают в блок ранжирования угроз, где формируется список актуализированных угроз, на которые необходимо обратить первоначальное внимание при построении или доработке АС – в отличие от стандартизированного подхода, который выдает список рекомендаций, полученных только на основе сравнения того, что требует стандарт и того, что формально присутствует в системе.

Для создания системы автоматизированной оценки защищенности АС разработан алгоритм, представленный на рис. 2.

Работа системы объединяет в себе 3 подхода к оценке и анализу защищенности АС: использование стандартизированного подхода; использование результатов работы СЗИ АС; использование интеллектуальных технологий.

Эффективное сочетание данных подходов позволит как предусмотреть требования стандарта 27001 [10], так и уйти от статичности требований стандарта и учесть прецеденты ИБ, что позволит более динамично управлять АС и с большей эффективностью оценивать защищенность.

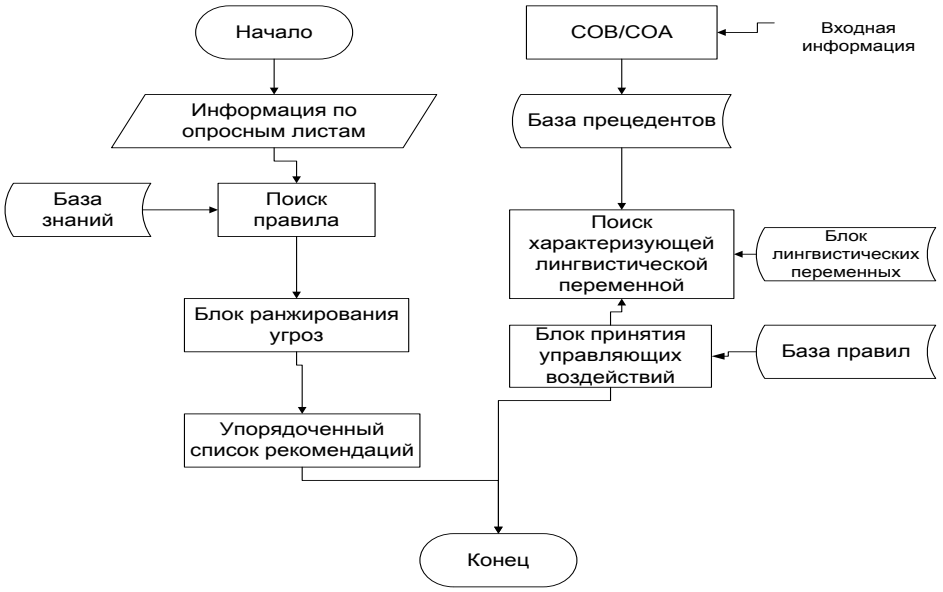

Рис. 2. Алгоритм работы автоматизированной системы на прецедентах оценки защищенности АС

Применение разработанного подхода позволяет уйти от субъективности (неопытности) пользователя, отвечающего на вопросы стандарта; использовать объективную информацию о наличие угроз ИБ АС, за счет автоматизированной обработки статистики по инцидентам; получить ранжированный список рекомендаций, которые необходимо выполнить для построения эффективной и удовлетворяющей требованиям стандарта системы защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.
2. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования. – Введ. 2000–30–06. – М.: Стандартинформ, 2001. – 22 с.
3. *Арьков П.А.* Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 30-36.
4. *Девянин П.Н.* Модели безопасности компьютерных систем: Учебное пособие для студ. высш. учеб. заведений. – М.: Изд. центр «Академия», 2005. – 144 с.
5. *Гончаров М.М., Борисов В.В.* Разработка модели анализа рисков информационной безопасности компьютерных систем на основе нечеткой логики // Научно-технический журнал «Защита информации». – 2011. – № 1 (18). Режим доступа: URL: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=18&pa=9&ar=1 (дата обращения 20.10.2013).
6. *Бородакий Ю.В, Добродеев А.Ю.* Проблемы и перспективы создания автоматизированных систем в защищенном исполнении // Известия ЮФУ. Технические науки. – 2007. – № 1 (76). – С. 3-6.
7. ГОСТ Р 51583–2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – Введ. 2000–06–04. – М.: Стандартинформ, 2001. – 20 с.
8. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 2006–27–12. – М.: Стандартинформ, 2008. – 26 с.

9. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – 2-е изд. перераб. – Киев: ООО «ТИД «ДС», 2008. – 286 с.
10. *Жукова М.Н. Золотарев А.В.* Применение нечеткой логики при решении задачи комплексной оценки защищенности автоматизированных систем // В мире научных открытий: научное периодическое издание. – 2011. – Вып. 12. – С. 205-214.

Статью рекомендовал к опубликованию к.т.н., доцент П.М. Гофман.

Жукова Марина Николаевна – ФГБОУ ВПО «Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева»; e-mail: mariem@inbox.ru; 660014, г. Красноярск, проспект им. газеты «Красноярский рабочий», 31; тел.: +79029101502; кафедра безопасность информационных технологий; к.т.н.; доцент.

Коромыслов Никита Андреевич – e-mail: koromyslov_nikit@list.ru; тел.: 83912621847; аспирант.

Zhukova Marina Nikolaevna – Siberian State Aerospace University; e-mail: mariem@inbox.ru; 31, prospekt imeni gazety «Krasnoyarskiy rabochiy», Krasnoyarsk, 660014, Russia; phone: +79029101502; the department of information technologies security; cand. of eng. sc.; associate professor.

Koromyslov Nikita Andreevich – e-mail: koromyslov_nikit@list.ru; phone: +73912621847; postgraduate student.

УДК 681.324

Ю.А. Брюхомицкий

МОДЕЛЬ АДАПТИВНОЙ САМООРГАНИЗУЮЩЕЙСЯ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ РЕШЕНИЯ ЗАДАЧ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ*

Рассматриваются новые подходы и принципы построения искусственной иммунной системы (ИИС), отличающейся от известных тем, что в ней воспроизводятся способности к адаптации и самоорганизации, присущие иммунной системе живых организмов. Предлагаются новые подходы к моделированию свойства двойной пластичности, основанные на использовании различных механизмов формирования и регулирования численности детекторов. В процессе функционирования ИИС детекторы градуируются по эффективности обнаружении «чужих». Также вводится механизм регулирования баланса способностей ИИС к обнаружению ранее встретившихся и новых «чужих». В конечном итоге функционирование ИИС проявляет свойства параметрической и структурной пластичности. Параметрическая пластичность реализуется на стадии предварительного обучения и заключается в выборе исходных параметров представления и кодирования информационных процессов, реализации процедуры создания шаблонов и формирования первичного набора детекторов. Структурная пластичность реализуется на стадии рабочего функционирования в «духе коллективизма» путем выявления и замены слабейших элементов новыми, удаления бесполезных элементов, заполнения ниш, не занятых имеющимися элементами. В конечном итоге в отличие от известных ИИС проявляет присущий живой иммунной системе комбинированный характер функционирования: экзогенный в части защиты от внешних нарушителей и эндогенный в части обеспечения постоянства и целостности внутренней среды и поддержания механизмов внутренней коммуникации.

Искусственная иммунная система; адаптация; самоорганизация; обнаружение «чужих» информационных процессов; свойства параметрической и структурной пластичности.

* Работа выполнена при поддержке гранта РФФИ 12-07-00081-а.