УДК 004.056.5

В.А. Михеев

МЕТОДИКА ВЫБОРА РАЦИОНАЛЬНОГО КОМПЛЕКСА ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ МНОГОФУНКЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Рассмотрена проблема выбора рационального состава системы защиты информации многофункциональной информационной системы холдинга. Предложен метод контурирования системы по категориям обрабатываемой информации. Обоснована необходимость использования метода морфологического синтеза программно-аппаратного комплекса защиты информации. Данный метод позволяет реализовать многокритериальный и многоальтернативный выбор. Разработана методика синтеза рационального программно-аппаратного комплекса защиты информации.

Информационная система; метод контурирования; система защиты информации; морфологический метод синтеза.

V.A. Mikheev

METHODS TO SELECT EFFICIENT HARDWARE-SOFTWARE SYSTEM FOR INFORMATION PROTECTION OF MULTIFUNCTIONAL INFORMATION SYSTEM

The article describes the problem to select efficient structure for information protection of corporation multifunctional information system. There proposed a method to contour a system as per category of processed information. The necessity to use a morphological synthesis method of hardware-software system for information protection is justified. The method enables implementation of multicriteria and multialternative selection. The methods of efficient hardware-software system synthesis for information protection have been developed.

Information system; contouring method; information protection system; morphological synthesis method.

Многофункциональная территориально распределенная информационная система (МИС) – взаимосвязанная совокупность кампусных локальных вычислительных сетей (ЛВС) и корпоративной сети передачи данных (КСПД), предназначенная для создания единого защищенного интегрированного информационного пространства информационных ресурсов предприятий холдинга. В связи с необходимостью циркуляции в МИС как общедоступной информации, так и информации ограниченного доступа, возникают требования по разработке системы защиты информации (СЗИ), а также особых подходов к проектированию и построению МИС как к автоматизированной системе в защищенном исполнении, отвечающей требованиям безопасности информации [1].

Разработка такой СЗИ может производиться на основе подходов и системотехнических принципов, сформулированных в [2, 3].

Учитывая территориальную распределенность МИС и существующие требования по защите информации, обоснованным решением при проектировании и

построении МИС является применение метода контурирования по категориям обрабатываемой информации [4].

Применение в МИС метода контурирования позволяет разбить МИС на три защищенных контура обработки информации (контуры безопасности), представленных на рис. 1:

- публичный информационный контур (ПИК) – выделяется для обработки, передачи и представления общедоступной информации в сетях международного информационного обмена (включая сеть «Интернет»);
- внутренний информационный контур (ВИК) – выделяется для обработки конфиденциальной информации, включающей коммерческую тайну, персональные данные и другие сведения, которые могут быть отнесены к конфиденциальным;
- защищенный информационный контур (ЗИК) – выделяется для обработки информации, содержащей сведения, составляющие государственную тайну.

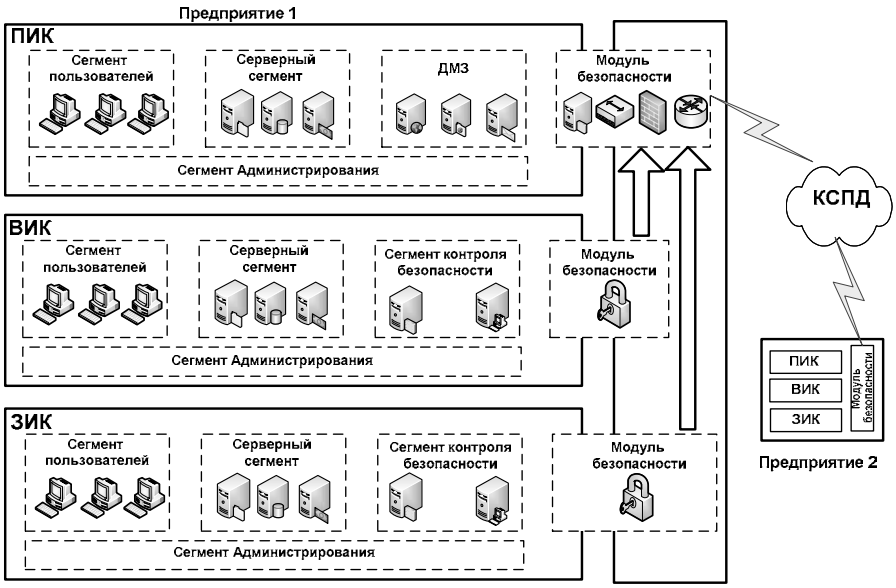

Рис. 1. Контуры обработки информации (контуры безопасности)

Объединение кампусных ЛВС предприятий холдинга в единое информационное пространство посредством КСПД происходит путем объединения контуров безопасности.

Угрозы, возникающие при таком объединении, решаются разработкой и внедрением в каждом контуре «модуля безопасности» – программно-аппаратного комплекса защиты информации (ПАКЗИ), обеспечивающего выполнение требований по защите информации (разных для каждого контура).

Публичный информационный контур обеспечивает доступ к публичным сервисам сети «Интернет». Требования по защите информации для ПИК регламентируются внутренними документами холдинга и обеспечиваются выполнением комплекса организационно-технических мероприятий. Подключение к сети «Интернет» осуществляется через модуль безопасности ПИК, при этом обеспечи-

вается организация «демилитаризованной зоны», в которой размещаются публичные ресурсы, такие как интернет-портал, почтовый сервер, DNS-сервер и др.

Внутренний информационный контур обеспечивает хранение, обработку и обмен конфиденциальной информацией. Требования по защите конфиденциальной информации для ВИК регламентируются руководящими документами ФСТЭК и ФСБ России и обеспечиваются комплексом организационно-технических мероприятий и проведением аттестации ВИК по требованиям защиты информации. В ВИК применяется целый ряд средств защиты информации (СрЗИ), позволяющих обеспечить требования по защите информации. Конкретный перечень СрЗИ определяется в соответствии с классификацией ВИК, проводимой на основании РД ФСТЭК России [5].

Защищённый информационный контур обеспечивает циркуляцию информации, содержащей сведения, составляющие государственную тайну. Требования по защите информации, составляющей государственную тайну, регламентируются руководящими документами ФСТЭК и ФСБ России, обеспечиваются комплексом организационно-технических мероприятий и проведением аттестации ЗИК по требованиям защиты информации.

В модулях безопасности ВИК и ЗИК применяются сертифицированные по требованиям безопасности информации программно-аппаратные комплексы криптографической защиты информации (шифраторы). Эти устройства выполняют функции шифрования, межсетевого экранирования, скрытия архитектуры защищаемого контура, тем самым обеспечивая требуемый уровень защиты контуров.

Любое взаимодействие между контурами безопасности до криптографического преобразования информации в модулях безопасности ВИК и ЗИК исключается путем физического разделения контуров. Потоки информации от всех трех контуров консолидируются в модуле безопасности ПИК, куда данные из ВИК и ЗИК поступают в зашифрованном виде, тем самым, исключая их компрометацию.

Необходимо отметить, что на сегодняшний день существует два подхода к обеспечению безопасности информации информационных систем [6,7]: фрагментарный и комплексный.

Фрагментарный подход направлен на противодействие строго определенным угрозам безопасности в заданных условиях функционирования МИС. Достоинством данного подхода является высокая избирательность к конкретной угрозе, а существенным недостатком – отсутствие единой защищенной среды обработки информации. Кроме того, даже небольшое видоизменение угрозы ведет к потере эффективности СЗИ.

Комплексный подход ориентирован на создание защищенной среды обработки информации в контуре, объединяющей в единый комплекс разнородные средства защиты информации (СрЗИ), образующие комплексную СЗИ. Комплексность СЗИ достигается охватом всех возможных угроз и согласованием между собой разнородных методов и средств, обеспечивающих защиту всех элементов контура. Достоинством данного подхода является возможность обеспечить требуемый уровень защищенности. К его недостаткам можно отнести наложение ограничения на свободу действий пользователей; сложность управления системой защиты; большая чувствительность к ошибкам установки и настройки элементов системы.

Однако за счет рационального построения СЗИ возможно свести недостатки данного подхода к минимуму.

Следовательно, в процессе проектирования модулей безопасности контуров МИС, состоящих из ПАКЗИ, необходимо решить задачу создания рационального выбора ПАКЗИ, с учетом совместимости всех СрЗИ, входящих в ПАКЗИ, для по-

строения комплексной СЗИ МИС, при наличии следующих ограничений: уровень защищенности, надежность, соответствие требованиям РД ФСТЭК России, наличие сертификата для класса АС, стоимость и т.д.

Совокупность ограничений вызывает необходимость использования многокритериального подхода для синтеза ПАКЗИ из множества альтернативных СрЗИ, удовлетворяющих этим ограничениям [8].

Решение задачи синтеза ПАКЗИ и, следовательно, построения комплексной СЗИ МИС усложняется рядом особенностей (необходимость учета большого числа показателей ПАКЗИ при оценке и выборе их рационального варианта, не только количественный, но и качественный (нечеткий) характер показателей и др.), которые делают практически невозможным применение традиционных математических методов, а также классических методов оптимизации для решения прикладных задач синтеза. Перспективным направлением разработки методов принятия решений является морфологический метод синтеза ПАКЗИ [9]. Данный метод позволяет реализовать многокритериальный и многоальтернативный выбор, в случае, когда ПАКЗИ реализуется из некоторого множества функциональных подсистем, при этом каждая подсистема имеет более одной альтернативы для её реализации.

В общем случае методика синтеза рационального ПАКЗИ, разработанная на основе предложенного метода морфологического синтеза, включает в себя следующие этапы:

Этап 1: компоновка вариантов синтезируемого набора СрЗИ для каждого контура в виде морфологической таблицы.

Этап 2: генерация всего множества возможных решений синтеза вариантов набора СрЗИ, отвечающих предъявляемым ограничениям.

Этап 3: выбор оптимального варианта (наилучшей альтернативы) по заданной целевой функции (принцип выбора).

Таким образом, предлагаемая в статье методика выбора рационального ПАКЗИ позволяет решить задачу построения комплексной СЗИ МИС как при наличии рассмотренных ограничений, так и других.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Михеев В.А.* Методология разработки и аттестации автоматизированных систем в защищенном исполнении // Материалы IX Международной научно-практической конференции «Информационная безопасность». – Таганрог, 2007.

2. *Михеев В.А.* Основы построения подсистемы защиты информации многофункциональной информационной системы // Известия ЮФУ. Технические науки. – 2008. – №8 (85). – С. 165 – 167.

3. *Николаев А.В., Михеев В.А.* Перспективы многофакторных систем // Защита информации INSIDE. – СПб, 2008. – Вып. 2. – С. 42 – 46.

4. *Михеев В.А.* Разработка модели безопасности многофункциональной информационной системы // Сб. трудов конференции “Перспектива – 2009”. – Таганрог, 2009. – С. 170 – 173.

5. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_docs/doc_3_3_004.htm. Дата обращения 01.09.2009.

6. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных: В 2-х кн. Кн. 1. – М.:Энергоатомиздат,1994. – 400 с.

7. *Сухарев Е.М.* Обеспечение информационной безопасности в экономической и телекоммуникационной сферах: Коллективная монография: В 3-х кн. Кн. 2. – М.: Радиотехника, 2003. – 216 с.

8. *Кащенко А.Г.* Задача многокритериального синтеза структуры и параметров системы защиты информации // Информация и безопасность: региональный научно-технический журнал. – Воронеж, 2006. – Вып. 2. – С. 107 – 110.

9. *Машкина И.В., Гузаиров М.Б.* Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Приложение к журналу «Информационные технологии». – 2008. – №7. – 2 с.

Михеев Вячеслав Алексеевич
Открытое акционерное общество «Концерн радиостроения “Вега”».
E-mail: mikheev@vega.su.
121170, г. Москва, Кутузовский проспект, 34.
Тел.: 8 (499) 2490585.
Заместитель директора.

Mikheev Viatcheslav Alekseevich
Joint-Stock Company «Radio Engineering Corporation “VEGA”».
E-mail: mikheev@vega.su.
34, Kutuzov avenue, Moscow, 121170, Russia.
Phone: 8 (499) 2490585.
The deputy director.

УДК 004.942 - 004.827

Г.А. Евстафьев

НЕЧЁТКИЕ КОГНИТИВНЫЕ КАРТЫ ПРИМЕНИТЕЛЬНО К УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается подход для управления рисками информационной безопасности на основе нечётких когнитивных карт и искусственных нейронных сетей. В подходе предлагается разделить понятия риска на две составляющие: системозависимый и системонезависимый риски. Данный подход позволяет уменьшить долю субъективизма при оценке риска информационной безопасности (ИБ) организации, учесть все элементы, участвующие и не участвующие в обработке данных в АС, и автоматизировать процесс управления рисками.

Управление рисками ИБ; нечёткие когнитивные карты; актив; сканеры безопасности.

G.A. Evstafiev

FUZZY COGNITIVE MAPS IN RELATION TO RISK MANAGEMENT INFORMATION SECURITY

The paper proposes an approach to risk management of information security based on fuzzy cognitive maps and artificial neural networks. In the approach proposed to divide the notion of risk into two components: a system-dependent and system-independent risks. This approach allows to reduce the proportion of subjectivity in assessing the risk of information security organization, consider all the elements involved and not involved in the processing of data in the Automatic Systems and automate the process of risk management.