УДК 663.1:004.056

И.Г. Дровникова[1], Е.А. Рогозин[2], А.А. Никитин[3]
([1]Воронежский институт МВД России, [2]Воронежский институт МВД России,
[3]В/Ч 28683; e-mail: idrovnikova@mail.ru)

МЕТОДИКА ПРОЕКТИРОВАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Разработана методика проектирования систем защиты информации от несанкционированного доступа в автоматизированных системах, которая позволяет получать количественные (обобщающие) показатели защищённости и разрабатывать программные комплексы оценки защищённости существующих и перспективных автоматизированных систем.

Ключевые слова: автоматизированная система, защита информации от несанкционированного доступа, количественный критерий защищённости, алгоритм количественной оценки защищённости.

I.G. Drovnikova, E.A. Rogozin, A.A. Nikitin

METHODS OF DESIGNING INFORMATION SECURITY SYSTEMS TO AUTOMATED SYSTEMS

The method of designing systems of information protection from unauthorized access to an automated system that allows obtain quantitative (generalized) indicators of security and develop software systems of the security assessment of existing and advanced automated systems is developed.

Key words: automated system, the system of information security against unauthorized access, a quantitative criterion of protection, the algorithm of quantitative security assessment.

Статья поступила в редакцию Интернет-журнала 14 марта 2016 г.

Введение и теоретическая часть

Как объект проектирования системы защиты информации от несанкционированного доступа (СЗИ НСД) автоматизированных систем (АС) представляют собой сложную организационно-программную систему, включающую различные программно-методические и программно-технические комплексы и характеризующуюся большим количеством разнородных параметров. Поэтому её создание требует разработки соответствующих математических моделей, алгоритмов и программных средств, предназначенных для разработки и повышения эффективности функционирования САПР СЗИ НСД АС [1].

В [2] был предложен способ вычисления количественного показателя защищённости АС и эффективности СЗИ НСД в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-2-2013 [3], содержащего полный аутентичный текст стандарта ISO/IEC 15408, разработанного Международным институтом стан-

дартов (ISO) и известного под названием "Общие критерии" ("Common Criteria"). Поэтому актуальной задачей для создания методики проектирования СЗИ НСД АС является разработка алгоритмов, реализующих указанную модель, чему и посвящена данная статья.

Научные результаты и их новизна

Разработана методика расчёта количественного критерия защищённости АС и эффективности СЗИ НСД, реализующая предложенную раннее математическую модель.

На основе разработанной в [2] математической модели определения и оценки количественного критерия защищённости АС предлагается соответствующий алгоритм (рис. 1).

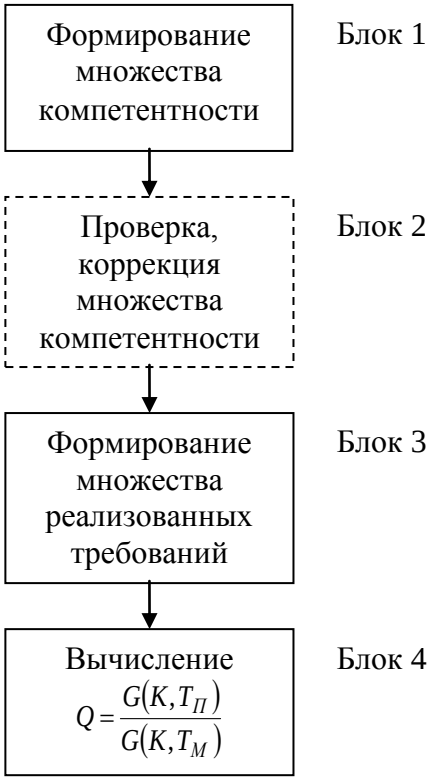

Рис. 1. Укрупнённая блок-схема алгоритма расчёта количественного критерия защищённости АС и эффективности СЗИ НСД

В блоке 1 осуществляется формирование множества компетентности *K*. При этом предполагается не проверка выполнения требований профиля защиты (ПЗ), а лишь берётся перечень компонентов требований "Общих критериев", упомянутых в профиле. Каждому компоненту требований из ПЗ ставится в соответствие направление компетентности из множества *K* независимо от того, является ли данный компонент конечным в иерархии компонентов своего семейства или же происходит разветвление указанной 0иерархии на более высоком уровне.

Если для оцениваемой АС нет подходящего ПЗ, то необходимо определить множество направлений компетентности, исходя из назначения АС, предполагаемых условий работы и т.д. При этом полученное множество требований должно быть проверено на соответствие идеологии "Общих критериев" (блок 2), в частности на удовлетворение зависимостей между компонентами и элементами требований.

В блоке 3 проверяется выполнение требований по каждому из заданных направлений компетентности. Определяется, требования компонентов какого иерархического уровня и с какими значениями параметров выполняются для данного направления компетентности.

В блоке 4 на основе результатов, полученных в блоке 3, вычисляют $G(K,T_{П})$, $G(K,T_M)$ и получают результат – количественный показатель защищённости Q в иерархическом дереве данных семейств, где $T_{П}$ – множество реализованных в системе требований, а T_M – множество максимальных требований, которые могут быть обоснованно предъявлены к рассматриваемой системе.

Функция $G(K,T_X)$ вычисляется исходя из равнозначности различных направлений компетентности. Для каждого направления $K_i \in K$ определяется степень выполнения требований от максимального уровня $G_i(T_X)$ в виде коэффициента со значением от 0 до 1. Затем эти значения суммируются:

$$G(K,T_X)=\sum_{K_i \in K} G_i(T_X). \qquad (1)$$

Очевидно, что если максимальное значение параметров требований $T_M = F(K)$, то $G_i(T_X)=1$ для всех $K_i \in K$, то есть значение $G(K,T_M)$ равно количеству элементов множества K.

$G_i(T_{П})$ определяется по формуле:

$$G_i(T_{П})=\frac{1}{J_i}\sum_{j=1}^{J_i} U_{ij}(T_{П})C_{ij}(T_{П}), \qquad (2)$$

где J_i – количество уровней иерархии в соответствующем направлении компетентности.

Функция $U_{ij}(T_{П})$ соответствует степени реализации требований j-го уровня. Если для данного направления компетентности нет иерархических разветвлений, то $U_{ij}(T_{П})$ принимает значение, либо 0 (требования соответствующего компонента не реализованы), либо 1 (требования реализованы). Если же имеются разветвления, то $U_{ij}(T_{П})$ принимает значение относительного количества компонентов j-го уровня, требования которых выполнены.

Функция $C_{ij}(T_П)$ определяет коэффициент значимости используемых параметров в отдельных элементах требований. Это значение аналогичным образом вычисляется как взвешенная сумма отдельных коэффициентов, характеризующих влияние тех или иных параметров. Учитываются параметры, входящие только в реализованные требования данного уровня, данного направления компетентности.

Блок-схема алгоритма вычисления $G(K,T_П)$ представлена на рис. 2.

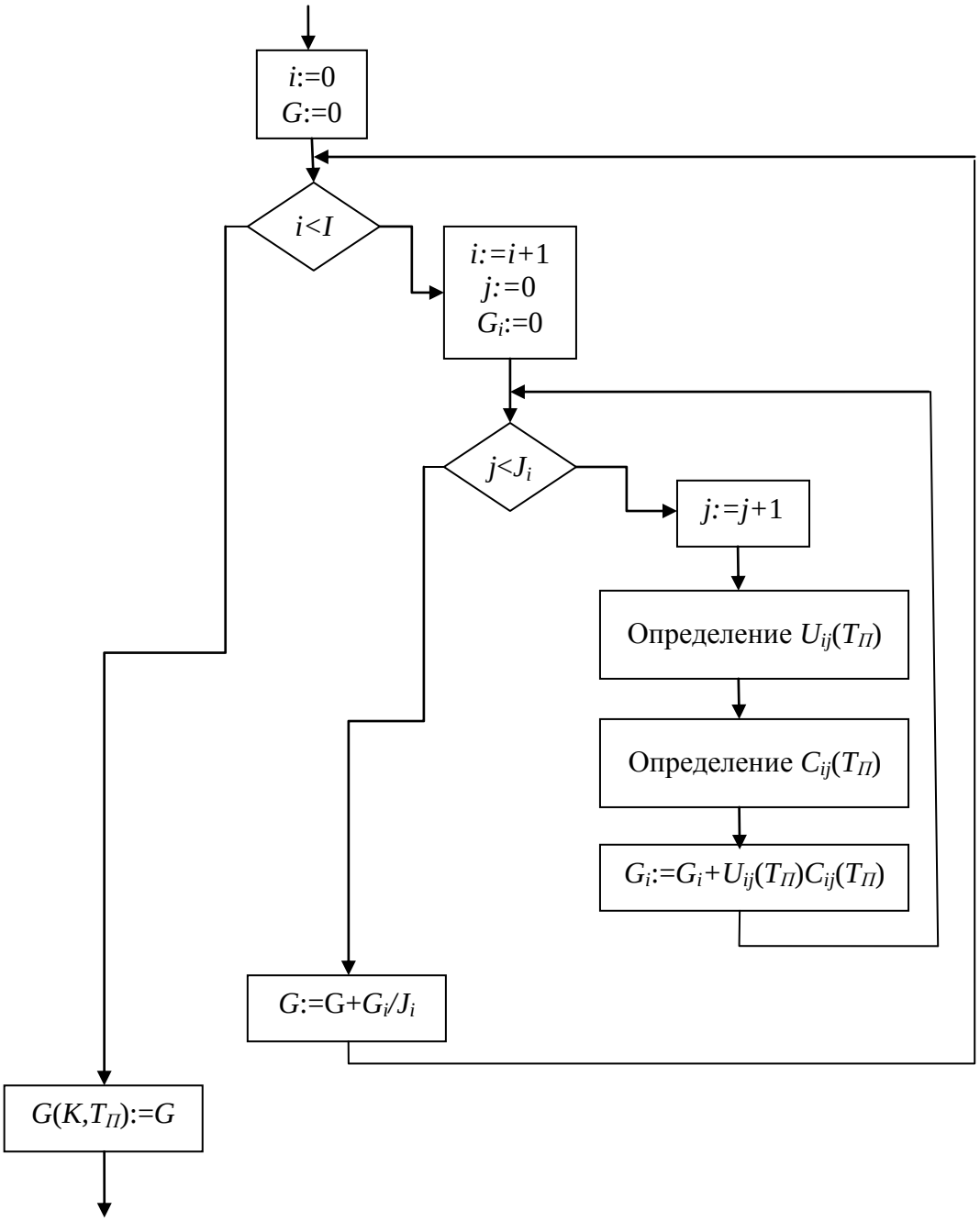

Рис. 2. Блок-схема алгоритма вычисления $G(K,T_П)$

Ниже приведены результаты практического применения предложенной методики проектирования СЗИ НСД, которые реализованы в форме программных средств, составляющих программное обеспечение (ПО) комплекса, поддерживающего автоматизированное выполнение процедур оценки защищённости АС.

Для облегчения работы с множеством функциональных требований ГОСТ Р ИСО/МЭК 15408-2-2013 были созданы база данных требований, а также программа PrCC, позволяющая добавлять, редактировать и просматривать содержимое этой базы данных.

Структура базы данных соответствует структуре функциональных требований. Заданы четыре таблицы: классов, семейств, элементов и компонентов. Таблицы взаимосвязаны с помощью ссылок принадлежности семейств соответствующим классам, компонентов – семействам, элементов – компонентам. Указанные зависимости используются в программе PrCC.

Оценка эффективности СЗИ НСД проводилась на основе количественного показателя, вычисляемого с помощью модели (2). В ходе определения значения количественного показателя были использованы проекты ПЗ, опубликованные на официальном сайте Федеральной службы технического и экспортного контроля (ФСТЭК) России. В частности, для определения множества компетентности K, а также производного от него множества $T_M = F(K)$ был использован ПЗ "Многоуровневые операционные системы в средах, требующих среднюю робастность". Данный ПЗ примерно соответствует третьему классу защищённости по руководящим документам ФСТЭК России. Требования использованного профиля были дополнены требованиями семейств FRU_PRS и FTA_TSE, поскольку их выполнение необходимо для эффективного администрирования системы, а именно для своевременного проведения мероприятий по предотвращению или прерыванию НСД.

В качестве направлений компетентности брались отдельные компоненты требований профиля. При этом, если в ПЗ был указан компонент, являющийся корнем иерархического разветвления, то ветви данного разветвления не рассматривались в качестве отдельных направлений компетентности.

Заключение

В статье предложена методика расчёта количественного критерия защищённости АС и эффективности СЗИ НСД.

Ценность предложенной методики состоит в том, что она позволяют получать количественные (обобщающие) показатели защищённости, что даёт возможность в дальнейшем разрабатывать программно-методические и программно-технические комплексы оценки защищённости как существующих, так и перспективных АС. В отличие от известных методик и способов, где оценка осуществлялась на основе логико-лингвистических моделей, не учитывающих динамические свойства СЗИ НСД, разработанная методика избавлена от данного недостатка.

Литература

1. ***Норенков И.П.*** Основы автоматизированного проектирования. М.: изд-во МГТУ им. Н.Э. Баумана, 2000. 360 с.

2. ***Дровникова И.Г., Никитин А.А., Змеев А.А.*** Способ вычисления количественного показателя защищённости автоматизированных систем на основе требований ГОСТ Р ИСО/МЭК 15408-1-2013 // Вестник Воронежского института МВД России. 2015. № 3. С. 82-86.

3. ***ГОСТ*** Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.