УДК 681.5.08;530.1

Ф.А. Самсонов[1]

ЛОГИКО-ПАРАМЕТРИЧЕСКИЙ ПОДХОД В ЗАДАЧАХ СИНТЕЗА СИСТЕМЫ КОМПЛЕКСНОГО КОНТРОЛЯ И АДАПТИВНОЙ ЗАЩИТЫ ПРИВИЛЕГИРОВАННЫХ МАССИВОВ ДАННЫХ

В настоящей статье представлена методика по решению задачи синтеза системы контроля и адаптивной защиты привилегированных массивов данных. Для решения поставленной задачи предлагается использовать логико-параметрический подход.

Ключевые слова: *автоматизированные системы управления, логико-параметрический метод, объект защиты.*

F.A. Samsonov

LOGICO-PARAMETRIC APPROACH TO THE PROBLEMS OF SYNTHESIS OF INTEGRATED CONTROL AND ADAPTIVE PROTECTION OF PRIVILEGED DATA

This article presents a methodology for solving the problem of synthesis of control systems and adaptive protection of privileged data. To solve this problem is proposed to use the logico-parametric approach.

Keywords: *automated management system, logico-parametric method, object of protection.*

В соответствии с принятой в Российской Федерации Доктриной информационной безопасности одной из основных задач национальной безопасности РФ является ведение активного противоборства угрозам функционирования критически важных государственных информационных структур. Особое место в перечне критически важных информационных структур занимают системы, обеспечивающие защиту особо привилегированных массивов информации в автоматизированных системах управления различного назначения.

Современные автоматизированные системы управления (АСУ ТП критически важных объектов, информационно-управляющие системы государственного назначения и т.п) являются сложными динамическими системами, функционирующими в гетерогенной программно-аппаратной среде, подверженной комплексному воздействию физических и информационных факторов эндогенной природы (порождаемых информационно-энергетическими процессами, протекающими внутри системы) и экзогенной природы (среда, человек, другие информационные системы). Информация о видах и характеристиках воздействий может являться неполной и/или недостоверной как в силу уникальности складывающихся условий обстановки, поведенческой неопределённости операторов, так и в силу неразличимости характеристик воздействия ввиду порождения вторичных (цепных) факторов. Особое место в перечне критически важных информационных структур занимают системы, обеспечивающие защиту привилегированных массивов данных в автоматизированных системах управления различного назначения [1].

В области моделирования и оценки защищённости сложных систем разработаны и применяются две основные методологии: детерминированная (нулевого риска) и вероятностная (ненулевого риска), которые способствовали расширению представлений об относительности безопасности и рождению концепции «приемлемого» риска. Оценка вероятностных показателей защищённости и риска получила развитие на основе «частотного» и «гипотетического» подходов, при этом в рамках «частотного» подхода констатируется фактическая реализация происшествий с отображением условий их возникновения. При «гипотетическом» подходе ис-

[1] Кандидат военных наук, доцент ФГБНУ «Экспертно-аналитический центр» при Минобразовании РФ.

пользуют гипотезы о функциях распределения вероятности о параметрах системы и характеристиках случайных процессов в ней. Следует отметить, что применительно к большим техническим и информационным системам использование такого подхода может сопровождаться методической погрешностью расчета вероятности, которая может превышать искомое истинное значение на несколько порядков. Кроме того, к трудностям и недостаткам применения используемых в детерминированной и вероятностной методологий для оценки риска уникальных систем можно отнести следующие:

− отсутствует статистика активных отказов или данных для обоснования характеристик гипотетических функций их вероятности;

− существуют сложности в определении и описании полной группы ситуаций в системе и, вследствие этого, оценка по экстремальным ситуациям может быть неполной и (или) недостаточно достоверной;

− признается неизбежность наличия приближенных и (или) недостоверных данных об объекте, нерегламентированных факторах и трактах их распространения и, тем не менее, отсутствуют методы, позволяющие а) учитывать нечеткую информацию, б) рассчитывать показатели безопасности и риска;

− отсутствуют общие модели для группы показателей «эффективность – безопасность – стоимость» с целью определения «приемлемого» риска и (или) обоснования их оптимального баланса;

− невозможность в рамках этих подходов нестатического нахождения мер определенности (неопределенности) реализации происшествия и самого нежелательного исхода (происшествия) в системе.

Таким образом, объективно существует научная проблема, заключающаяся в разработке моделей и методов синтеза системы комплексного контроля и адаптивной защиты АСУ, обеспечивающей гарантированную защищённость динамической информации в условиях неполноты и недостоверности сведений о видах эндогенных и экзогенных угроз.

Методологической основой научного исследования являются работы [1–11], в частности следующие положения:

− утверждение Поспелова – Клира – Прада о соотношении вероятностной и возможностной мер наступления сложного события или возникновения процесса [3];

− предположение о полноте лингвистического и множественно-параметрического описания свойства «безопасность – опасность» системы [4];

− гипотеза о соответствии событийного и множественно-параметрического способов моделирования предпосылок опасности [5; 9; 11].

Предлагаемый логико-параметрический подход [4; 6; 12] предполагает в своей основе: а) допустимость описания причинно-следственной связи реализации угрозы системе в виде совокупности частных логических (булевых) функций связности источника воздействия, нелегитимного канала распространения воздействия, приёмника воздействия и защитных функций ослабления воздействия; б) формирование обобщённой функции связности конечного (критического) события как аддитивной функции элементарных исходов частных функций в логической модели вида «угроза – защита – объект» и параметрической модели вида «воздействие – ослабление – восприимчивость»; в) возможности представления и количественной оценки защищённости объекта как результата действий видов факторов экзогенной (внешних по отношению к системе: рабочая среда, человек-оператор) и эндогенной (внутри) природы, характеристических функций защиты и характеристик собственной резистентности объекта защиты к фактору в параметрической модели вида «воздействие – ослабление – восприимчивость»; г) синтеза рациональной структуры и функционала системы контроля и защиты на основе квазиоптимального плана распределения ресурсов защиты по критерию значимости риска угрозы; д) адаптивное по критерию «оперативность – ресурсоёмкость» управление уровнем защищённости динамической информации в АСУ.

Последовательность этапов

1. На основе анализа морфологической и функциональной моделей системы, характеристик эндогенных и экзогенных факторов (в общем случае – нечётких величин) формируется направленный граф возможных состояний. Предполагается, что в системе текущее (исходное) состояние характеризуется мерой защищённости $z\ (t, v, f, r)$ как функцией от параметров видов воздействий v и собственной восприимчивостью к соответствующим воздействиям r объектов защиты, а также функций ослабления воздействий f множеств средств защиты, при этом возможность реализации угрозы, как переход системы из состояния $zt > zt_{доп}$ в критическое $zt = zt_{доп}$ и (или) надкритическое состояние

$zt < zCr$, $z \to Cr$, – их нечеткими областями существования. Требуется при стоимостных $\$ \le \$_{зад}$ и временных $\tau \le \tau_{тр}$ ограничениях установить возможностную меру $\pi(\zeta)$ перехода $z \to Cr$ этой системы в критическое состояние (определить параметры функции реализации угрозы):

$$\pi(z \to Cr) = \text{Pos}\,(\text{F}\,(\text{V}) \cap \text{R} \neq \varnothing \mid \text{V}\, iCr \subseteq \text{VAC}). \quad (1)$$

Формально (в узком смысле) по [3; 10] возможностная мера $\pi(\zeta)$ – это степень принадлежности значений переменной λ нечеткому множеству Λ, определяемая по функции принадлежности $\mu\Lambda(\lambda)$; в широком смысле мера – асимптота вероятностной меры события.

2. На основе возможностных мер реализации вершинного (критического) события – реализации угрозы объекту (~там) защиты ($\pi(zCr)$) и значений функций ущерба ui от реализации такой угрозы – определяются соответствующие риски объекта защиты ($Ri = \pi(zCr)ui$); проводится их ранжирование.

3. В целях определения рациональной структуры системы контроля и защиты на основе рассмотрения логической модели функций связности и параметрической модели «воздействие – восприимчивость» формируется логико-параметрическая модель фреймовой сети; определяется множество нечётких параметров $(f, \mu(f))$, описывающих характеристики ресурсов системы защиты; определяются целевые параметры xj объектов защиты (на основе ранжированных рисков) и соответствующие величины отклонения ($-\delta xj$) – от расчётного запаса безопасности параметра. В процессе управления целевым параметром xj – с целью ликвидации отклонения ($-\delta xj$), множество возмущенных неуправляемых переменных $\{xBj.n\}$ исключается из процесса оптимизации. В этом случае процесс обеспечения устойчивости параметра xj состоит в выборе такого управления u, которое бы обеспечивало за счет изменения множества управляемых параметров $\{xyj.u\}=\{x\} - \{xBj.n\}, \{x\}=\{xj.1, \ldots, xj.m\}$ искомую компенсацию ($-\delta xj$). Применение описанного метода даёт возможность произвести учет ресурсных затрат (временных, материальных) на реализацию изменения той или иной совокупности параметров управления. Действительно, вводя соответствующие нормирующие (по видам ресурсов) множители λjuk и задавая величину ресурса βk на проведение k-й совокупности мероприятий (общим числом m), дополнительно имеем систему уравнений – ограничений вида:

$$J^0 \begin{cases} \sum\limits_u \gamma_{ju1} \delta x_{ju} = \beta_1 \\ \sum\limits_u \gamma_{ju2} \delta x_{ju} = \beta_2 \\ \ldots \\ \sum\limits_u \gamma_{jum} \delta x_{ju} = \beta_m . \end{cases} \quad (2)$$

4. Адаптивный выбор стратегии управления ресурсами защиты на основе критерия «оперативность – ресурсоёмкость» $K^*=((Kz(u^*),t,c), K2(u^*), \ldots, Km(u^*))$, где u^* – любая стратегия из UL возможных:

$$K_z(u^*) = \underset{u \in U}{lex} \min K_z(u,t,c). \quad (3)$$

Таким образом, логико-параметрическое описание причинно-следственных связей и характеристик воздействий факторов на объект защиты позволяет выразить интегральную возможностную меру возникновения исследуемого исхода на комплексе элементарных мер с накоплением причин и предпосылок опасности. При рассмотрении событий (реализаций предпосылок и функций опасности) в физическом аспекте и выражении их в нечетком множественно-параметрическом виде становятся очевидными методы и модели определения возможностной меры их возникновения, а в формальном плане – ясными правила оперирования с ней.

Детально предлагаемый логико-параметрический подход представлен в [6; 9], особенности реализации методов синтеза и формально-логические модели комплексной системы контроля и адаптивной защиты приведены в [7; 8].

Литература

1. Ловцов Д.А. Управление безопасностью эргасистем. – М. : ВА РВСН, 2000. – Ч. 1. – 172 с.

2. Глазов Б.И. Системология информационных отношений в сфере управления : монография. – М. : ВА РВСН им. Петра Великого, 2005. – 244 с.

3. Дюбуа Д., Прад А. Теория возможностей. Приложения к представлению знаний в информатике – М. : Мир, 1989. – 286 с.

4. Есипов Ю.В, Самсонов Ф.А., Черемисин А.И. Мониторинг и оценка риска систем «защита – объект – среда» : монография. – М. : Издательство ЛКИ, 2008.–136 с.

5. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб.: Политехника, 2000. – 248 с.

6. Самсонов Ф.А. Комплексная оценка безопасности информационно-вычислительных систем : монография. – М. : ВА РВСН, 2012 – 144 с.

7. Самсонов Ф.А. Безопасность автоматизированных систем специального назначения: факторный параметрический подход. // Вопросы защиты информации. – 2013. – № 2. – С. 78–81.

8. Самсонов Ф.А. Модель и метод рационального распределения ресурсов АСУ СН для противодействия многофакторной угрозе // Коммуникационные технологии и сети (CTN-2013). – М. : МТУСИ, 2013 – С. 147–150.

9. Гладышев А.И. Разработка имитационной модели вирусной эпидемии на основе модели биологических вирусов: принципы, основные параметры, описание и зависимости // Вестник Российского нового университета. – 2012. – Выпуск 4 : Управление, вычислительная техника и информатика.– С. 17–21 .

10. Гладышев А.И., Жуков А.О. Использование в автоматизированной системе контроля полномочий биометрической идентификации // Вестник Российского нового университета. – 2013. – Выпуск 4 : Управление, вычислительная техника и информатика. – С. 95–99.

11. Гладышев А.И. Удобство и безопасность компьютерных систем, в чем противоречие // Вестник Российского нового университета. – 2012. – Выпуск 4 : Управление, вычислительная техника и информатика. – С. 89–93.

12. Гладышев А.И., Жуков А.О. Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. – 2013. – Выпуск 4 : Управление, вычислительная техника и информатика. – С. 53–56.