КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 004.7:004.056

В.А. МАРЧЕНКО

ФОРМАЛИЗОВАННАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Введение. Одной из наиболее активно исследуемых направлений в информационной безопасности является задача оптимального синтеза систем защиты информации (СЗИ). Это объясняется повышением требований к эффективности, качеству и надежности систем, увеличением числа и объема информационных массивов, сложности и стоимости разработки и отладки таких систем, переходов от разработки простых и слабо связанных СЗИ к комплексным решениям для защиты всей информационной среды [1]. Учитывая отсутствие развитой формальной методологии разработки и проектирования СЗИ эта задача является много затратной.

Существует много рекомендаций по созданию отдельных типов устройств их оптимизации под выполняемые задачи и последующее объединение в единую систему защиты. Но все они имеют недостаток в виде ориентации на определённое множество задач и не являются универсальными. Учитывая это, появляются все новые и новые устройства для защиты зачастую не имеющие, каких либо уникальных качеств и характеристик с точки зрения безопасности, и решающие задачи защиты информации только в определённой информационной среде. При разработке таких средств очень мало уделяется внимание вопросам взаимодействия отдельных СЗИ в единой системе, их влияние друг на друга и тому подобное.

Постановка задачи. Такая малая освещённость обуславливается ранее существовавшей практикой создания единой системы

V.A. Marchenko

THE FORMALIZED TECHNOLOGY OF DESIGNING OF SYSTEMS OF THE INFORMATION PROTECTION

In article problems of creation of the formalized technology of designing of systems of protection of the information are considered. Concepts FS and SFS as constructive elements of systems of safety are entered, the simplified mathematical model is resulted, and also directions of the further scientific researches are given

Рассмотрены вопросы создания формализованной технологии проектирования систем защиты информации. Введены понятия функция безопасности и элементарная функция безопасности как конструктивных элементов систем безопасности, приведена упрощённая математическая модель, а также определены направления дальнейших научных исследований.

защиты из существующих разрозненных элементов, где к уже существующей информационной среде добавляются СЗИ. Современные условия диктуют другой подход, который заключается в том, что изначально вся информационная среда проектируется с точки зрения защиты всех её компонентов. Это предполагает возможность оценить ещё на этапе проектирования целесообразность использования того или иного СЗИ, а также промоделировать их взаимодействие в едином информационном взаимодействии.

Поэтому главной задачей данной работы является анализ и формализация методики проектирования СЗИ на основе использования понятий – функция безопасности (ФБ) и элементарная функция безопасности (ЭФБ).

Состояние проблемы. Создание формальной методологии проектирования СЗИ сопряжено с рядом трудностей, которые объясняются: сложностями структуризации систем; как правило, большим числом изменений в постановках задач, определении требований и детальных спецификаций в ходе разработки; сложностью внедрения формальных методов и автоматизации проектирования; трудностями выработки и принятия стандартов на интерфейсы и форматы данных, а следовательно, сложностью обеспечения интероперабельности систем и подсистем, их адаптируемости к вновь возникающим задачам и к различным условиям функционирования, переносимости с одной аппаратной платформы на другую [2]. Данная задача решается несколькими методами один, из которых заключается в создании многоагентной модели системы защиты компьютерной сети, состоящей из набора автономных интеллектуальных агентов, распределенных по объектам защищаемой информационной среды и кооперирующихся с целью принятия совместных непротиворечивых решений [3]. К недостаткам такого решения относят трудность практической реализации конечного продукта, а также необходимость создания общей системы принятия решения, которое тоже является нетривиальной задачей.

Другим широко используемым подходом решения данной задачи является создание СЗИ из готовых существующих компонентов, но с применением разных оптимизирующих методик [4, 5]. Эти методики основываются на решении многокритериальной задачи выбора оптимального комплекса СЗИ.

Третьим подходом можно считать создание СЗИ с использованием международного стандарта называемого «Общие критерии» [6]. Однако этот стандарт больше ориентирован на разработку отдельного устройства защиты с последующей оценкой соответствия его данным критериям. Другой явный недостаток – большая формализация оценки, что не позволяет оценить разные СЗИ относящиеся к одному классу оценки.

Схожий подход используется в технологии, которая предложена автором [7] и названа модульной.

Методы решения задачи. Используем некоторые понятия теории множеств и математической логики [8]. Пусть A конечный алфавит, A' — множество слов конечной длины в алфавите A. Из A с помощью некоторых правил выделено подмножество L правильных слов, которое называется языком. При этом

$$A' >> L \text{ и } L \subseteq A'.$$

Если L_1 – язык описания одной информации, L_2 – другой информации, то можно говорить о языке L, объединяющем L_1 и L_2 описывающем ту и другую информацию. Тогда L_1 и L_2 подъязыки L.

Будем считать, что любая информация представлена в виде слова в некотором языке L. Кроме того, можно полагать, что состав любого устройства в вычислительной системе достаточно полно описано словом в некотором языке. Тогда можно отождествлять слова и состав устройств и механизмов вычислительной системы или произвольной электронной системы обработки данных. Эти предположения позволяют весь анализ вести в терминах некоторого языка.

Объектом относительно языка L называется произвольное конечное множество языка L. Объект, производящий преобразование называется **субъектом**. Согласно аксиомы положенной в основу американского стандарта по защите «Оранжевая книга» в [9] все вопросы безопасности информации описываются доступами субъектов к объектам.

Под угрозой вычислительной системе будем понимать возможность осуществления неразрешённого доступа объекта к субъекту. Существуют следующие классы угроз [10]: угроза раскрытия*;* угроза целостности*;* угроза отказа в обслуживании.

СЗИ будем называть любой программно-аппаратный комплекс, предназначенный для целей защиты информации.

В общем случае ФБ – это любая последовательность информационных воздействий предотвращающих выполнение какой-либо угрозы или сводящих выполнение угрозы к минимальным последствиям. Для реализации функции безопасности должна быть построена система, имеющая следующую математическую модель:

$$I_e = F(f', I_b),$$

где F – функционал, реализующий определенные преобразования; $f' = \{f_0, f_1, .., f_n\}$ – упорядоченное множество входных параметров безопасности, реализованных внутри системы; I_b, I_e – входной и выходной информационный поток соответственно. Эта модель интерпретируется графической схемой, показанной на рис. 1.

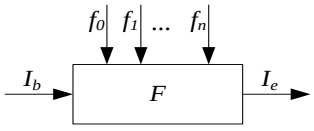

РИС. 1. Графическая интерпретация понятия ФБ

Если ФБ некоторое конечное множество слов C языка B, то ЭФБ являются алфавитом языка B. Обозначим его A из которого с помощью определённых грамматических правил G выводятся слова принадлежащие языку B .

$$C = G(A) \subset B.$$

В таком случае ЭФБ будет иметь такой вид:

$$I_e = F(f, I_b),$$

графически это интерпретируется (рис. 2):

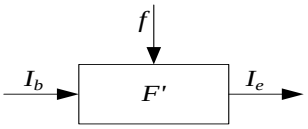

РИС. 2. Графическая интерпретация понятия ЭФБ

На рис. 2 F' – подсистема, реализующая единственную функцию, f – входной параметр безопасности реализованной внутри системы.

Множество возможных ЭФБ является конечным в конкретный момент времени, но с развитием технологий могут появляться как новые угрозы, так и новые ЭФБ соответственно. Особенностью ЭФБ является дальнейшая неделимость с точки зрения безопасности. Так как после разделения ЭФБ на составные части она теряет свои начальные свойства ЭФБ и представляет собой набор компонентов выполняющих определённые функции несвязанные с безопасностью.

Исходя из определения ЭФБ можно описать некоторые свойства взаимодействия между ними:

- объединение ЭФБ – при объединении ЭФБ между собой получается следующая система, показанная на рис. 3.

$$I_e = F(\bigcup_{n=0,..k} F'_n, I_{bn}),\ k \text{ – целое число.}$$

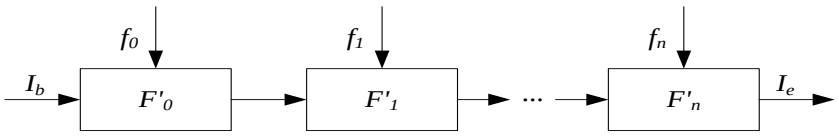

РИС. 3. Схема объединения ЭФБ

Выполняя операцию объединение между ЭФБ в конечном результате получается цепочка ЭФБ, в которой каждый элемент выполняет свое преобразование, но в совокупности не порождают новую систему со своими свойствами. В терминах формальных языков описывается как

$$C = G(A) \not\subset B.$$

Тогда формальная модель построения объединения ЭФБ будет такой системой:

$$I_e = (\bigcup_{n=0,..,k} F'_n, I_{bn}),$$

$$F' \in C \mid C = G(A) \not\subset B;$$

- интеграция ЭФБ – при интеграции ЭФБ между собой получается реализация конкретной ФБ. Формальная модель построения ФБ представляет собой

$$I_e = F(F'', I_b),$$

$$F'' = \{F' \in C \mid C \in G(A) \subseteq B\}.$$

При выполнении операции интеграции между ЭФБ в конечном результате получается новая система, имеющая набор новых уникальных функций и свойств которыми не обладают исходные ЭФБ.

С точки зрения безопасности удобно оперировать с ФБ так как они обладают некоторым набором уникальных свойств и могут использоваться в конечных системах без изменения.

В вышеприведенных моделях не детерминированным элементом является множество неправильных и правильных грамматик *G*. Поэтому создание автоматической системы проектирования всевозможных ФБ не представляется возможным. Но создание системы проектирования и анализа СЗИ использующих некоторый заданный набор готовых ФБ является вполне реальной задачей.

Практические результаты. Создание СЗИ с использованием предложенной технологии имеет следующий вид:

пусть T_i – множество угроз целостности; T_o – множество угроз раскрытия; T_d – множество угроз отказа в обслуживании, причем

$$T_i \cap T_o \cap T_d = \varnothing.$$

Положим, что время *t* дискретно, тогда S_t – множество субъектов в момент времени *t*, O_t – множество объектов в момент времени *t:*

$$T^t \le T_i \cup T_o \cup T_d.$$

T^t – множество угроз целостности раскрытия и отказа в обслуживании действующих на S_t в момент времени *t*, тогда в каждый момент времени *t* на информационную систему представленную множеством S_t действует множество угроз T^t.

$$O_t \xrightarrow{T^t} S_t.$$

Для предотвращения выполнения T^t должны быть реализованы соответствующие ЭФБ в виде готовых ФБ. В общем случае $O_t \neq const$, при $t = 1\ldots\infty$, тогда и $T^t \neq const$ при $t = 1\ldots\infty$.

Таким образом, перед разработчиком систем безопасности становится проблема создания набора ФБ для защиты S_t от выполнения T^t при $t = 1\ldots\infty$. Для решения этой задачи используется следующий метод: из каждого множества T_i, T_0, T_d, выделяется подмножество с наиболее большим показателем вероятности.

В общем случае СЗИ реализует два множества ФБ: *P* – множество основных ФБ предназначенных для решения целевых задач СЗИ; *S* – множество дополнительных ФБ предназначенных для решения нецелевых задач СЗИ.

$$M = P \cup S.$$

Множество *M* состоит из всех ФБ реализованных в конкретном СЗИ. На защищаемую систему действует множество угроз T^t, для защиты должно выполнятся условие:

$$T^t \cap M = \varnothing,$$

т. е. для всего T^t должно быть реализовано *M*. В принципе для конкретного времени *t* эта задача решается полностью. Но если учесть, что $|M| = const$, а $|T| \neq const$, с течением времени, то для решения задачи защиты должно выполнятся условие:

$$\left|M\right| > \left|T^t\right|.$$

Это в общем случае позволяет предусмотреть возможное появление дополнительного подмножества угроз, для которых уже реализовано ФБ. В реальных СЗИ такой подход с одной стороны приводит к значительному усложнению СЗИ, учитывая, что нет гарантии, что эти дополнительные ФБ, когда-нибудь, будут полностью задействованы. С другой стороны удорожает само СЗИ для конечного потребителя. Поэтому, для увеличения экономического эффекта, возможным представляется использование следующего соотношения:

$$\left|M\right| = \left|T^t\right|.$$

Таким образом, для защиты от дополнительного подмножества угроз появившимся с течением времени *t* следует заменить имеющееся СЗИ на другое где реализованы необходимые ФБ.

В качестве альтернативы создания СЗИ, автором предложена модульная архитектура [7], имеющая следующие особенности:

- имеется набор модулей СЗИ, каждый из которого реализует фиксированный набор ФБ;
- каждая существующая ФБ реализуется в единственном модуле СЗИ и не повторяется больше ни в каком другом.

Тогда каждый модуль СЗИ реализует только множество *P* и не реализует множество *S*, которое реализуется как основное множество *P* в другом модуле. Согласно ранее указанным отношениям на защищаемую систему действует множество потенциально возможных угроз. Но благодаря модульной архитектуре СЗИ выполняется следующее соотношение:

$$\left|M_1 \cup M_2\right| \geq T, \text{ где } M_1 \cap M_2 = \varnothing.$$

M_1 – множество реализованных ФБ первым модулем, M_2 – множество реализованных ФБ вторым модулем.

Такое решение имеет определённые недостатки в виде возможно не используемых ФБ второго модуля СЗИ но, оно гарантирует минимальную избыточность ФБ, а также лёгкую расширяемость ФБ без значительных трудозатрат и капитальных вложений как со стороны производителя СЗИ, так и со стороны пользователя.

Заключение. Введенные понятия ФБ и ЭФБ как конструктивные элементы систем безопасности являются перспективными для дальнейшего развития фор-

мализации процесса разработки конечных продуктов. Существует множество методик оптимизации создания СЗИ в [10], или предлагающих типовые шаблоны для типовых организаций в [11]. Предложенная технология позволяет наиболее эффективно выбрать множество СЗИ для реализации заданной политики безопасности внутри организации.

В дальнейшем предполагается разработка математической модели оценки эффективности и оптимальности реализации конкретных ФБ в СЗИ. Другим направлением исследований является моделирование СЗИ с использованием сетей Петри в [12]. На основе этой модели планируется создание методики оценки защищённости системы, а также оптимальности использования готовых СЗИ для целевой защищаемой системы.

Использование формальных методик создания СЗИ позволяет перейти на качественно новый уровень проектирования таких систем в [13]. Что в свою очередь значительно увеличивает защищенность, как всей информационной среды, так и отдельных её компонентов.

1. *Хоффман Л.Дж*. Современные методы защиты информации: Пер. с англ. ─ М.: Сов. радио, 1980. ─ 264 с.
2. *Яблонский А.С*. Формальная методология проектирования открытых систем // Тр. X Междунар. конф. «Проблемы управления безопасностью сложных систем». ─ М.: ─ 2002. ─ **2.** ─ С. 140 ─ 142.
3. *Городецкий В.И., Карсаев О.В., Котенко И.В., и др.* Многоагентная модель защиты компьютерной сети: Демонстрационный пример // Proceedings of the International Workshop Mathematical Methods, Models and Architectures for Computer Network Security. Lecture Notes in Computer Science. ─ 2001. ─ Vol. 2052, Springer Verlag. ─ P. 39 ─ 50.
4. *Теренин А.А.* Проектирование экономически эффективной системы информационной безопасности // Защита информации. INSIDE. ─ 2005. ─ № 1. ─ С. 2 ─ 11.
5. *Васильев В.И., Иванова Т.А.* Алгоритм проектирования оптимальной структуры комплексной системы защиты информации на основе анализа риска // Информационное противодействие угрозам терроризма. ─ 2005. ─ № 6.─ С. 3 ─ 16.
6. *Evaluation* Criteria for IT Security. ─ ISO/IEC 15408─1: 1999. ─ 52 p.
7. *Алишов Н.И., Марченко В.А*. Технология интеграции средств защиты сетевого периметра // Математические машины и системы. ─ 2006. ─ № 2. ─ С. 36 ─ 47.
8. *Кук Д., Бейз Г.* Компьютерная математика. ─ М.: Наука, 1990. ─ 384 с.
9. *National* Computer Security Center. Trusted Network Interpretation. ─ NCSC-TG-005, 1987. ─ 332 p.
10. *Бутенко Д.В., Бутенко Л.Н.* Теория развития систем, задачи концептуального проектирования и их взаимосвязь с закономерностями развития систем // Качество. Инновации. Образование: Ежеквартальный научно-практический журнал. ─ 2004. ─ № 1.─ С. 38─41.
11. *Грушо А., Тимохина Е.* Теоретические основы защиты информации. ─ М.: Яхтсмен, 1996.─ 188 с.
12. *Котов В.Е.* Сети Петри. ─ М.: Наука, 1984. ─ 160 с.
13. *Снапелев Ю.М., Старосельский В.А.* Моделирование и управление в сложных системах. ─ М.: Советское радио, 1974. ─ 354 с.

Получено 30.01.2007