2004. – Вип. 2. – С. 172-180. ***27.*** *Яковлев С. В., Торяник В. В. Стратегия глобализации корпоративных информационных систем на базе новейших микрокомпьютерных технологий. -Радиоэлектроника и информатика.- 2004.- № 2.- С.126-131.* ***28.*** *Ансоф И. Стратегическое управление. - М.: Экономика, 1989.- 519 с.* ***29.*** *Каныгин Ю. М., Калитич Г. И. Основы теоретической информатики. - Киев: Наук. думка, 1990. - 232 с.* ***30.*** *Дружинин В. В., Конторов Д. С. Проблемы системологии (проблемы теории сложных систем). - М.: "Советское радио", 1976.- 296с.* ***31.*** *Словарь по кибернетике под. ред. В. М.Глушкова. К.: Глав. ред. укр. сов. энциклопедии К.: 1979.– 359 с.* ***32.*** *Проектування інформаційних систем. Посібник. За ред. В. С. Пономаренка К.: Вид. Центр "Академія", 2002. - 486 с.* ***33.*** *Інформаційні системи і технології в економіці. Посібник. За ред. В. С. Пономаренка К. Вид. Центр "Академія", 2002. - 542 с.* ***34.*** *Холл А. Д. Опыт методологии для системотехники. Пер. с англ. Под ред. Г. Н. Поварова. М., "Сов. Радио", 1975.- 448 с.* ***35.*** *Каныгин Ю. М., Гулеватый В. Г. ЭВМ: социально-экономические функции. Сер.Ш: "Экономика: наука, управление, практика" Общ. "Знание" УССР № 6. К.: Знание, 1985. - 49 с.* ***36.*** *Каныгин Ю. М. Индустрия информатики. К.: Техника, 1987.- 152 с.* ***37.*** *Петров Э. Г., Новожилова М. В., Гребенник И. В., Соколова Н. А. Методы и средства принятия решений в социально экономическких и технических системах. Учебное пособие / Под общ. Ред. Э. Г. Петрова - Херсон: ОЛДІ-плюс, 2003. –380 с.* ***38.*** *Глушков В. М., Каныгин Ю. М. Основы экономики и организации машинной информатики. К.: ИК, 1981.– 64 с.* ***39.*** *Pocket PC экономит $1 млн. в год / www.mconline.ru/post/20513/default.asp*

УДК 681.3

АНАЛИЗ СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ С ПОЗИЦИИ ЦЕЛЕНАПРАВЛЕННОГО ДЕЙСТВИЯ

Сергей Ливенцев
Специальный факультет СБ Украины ВИТИ НТУУ «КПИ»

Аннотация: **Рассмотрены проблемы управления системами защиты информации с точки зрения системного подхода. Показано, что подход к определению системы управления с позиции целенаправленного действия позволяет рассматривать требования по защите информации как аксиоматическую группу суждений.**
Summary: **The article examines the problems of management by the systems of defence of information from point of systems approach. It is shown that approach to determination of the control system from position of purposeful action allows to examine the requirements on defence of information as the axiomatic group of judgements.**
Ключевые слова: **Система управления, целенаправленное действие, система защиты информации**.

I Введение

Система безопасности – постоянно осуществляемый комплекс мер по предупреждению, пресечению и ликвидации последствий максимального количества угроз из полного набора возможных угроз для данного объекта или системы в целом [1]. Системный подход к анализу систем безопасности и системное исследование представляют собой естественный и, наверное, единственный научный метод решения теоретических и практических задач обеспечения защиты информации.

В арсенале общего системного исследования имеется [2], во-первых, теория абстрактных систем, а во-вторых, теория конкретных систем, включающая методологию анализа и синтеза. При выполнении конкретных системных исследований систем защиты информации (СЗИ) достаточно часто дается приоритет или теории абстрактных систем, или теории конкретных систем. Антагонизм теорий проявляется уже в самом определении системы как таковой. Так, в теории абстрактных систем за нее принимается множество взаимосвязанных элементов системы, которые по своей сути являются понятиями. Теория же конкретных систем определяет СЗИ как множество взаимосвязанных элементов, которые обладают свойствами физических объектов. В то же время допустимо считать, что теория управляемых систем может иметь единую общую исходную точку, определяемую с помощью понятия «целенаправленное действие» [3]. Гипотеза о связанности теорий абстрактных и конкретных управляемых систем позволит ввести в системное исследование абстрактных СЗИ общие принципы методологии анализа и синтеза конкретных систем.

II Постановка задачи

Безопасность – состояние объекта защиты, при котором организовано максимально возможное

противодействие дестабилизирующим факторам (угрозам) как на этапе предупреждения и пресечения, так и на этапе ликвидации последствий от их реализации [3]. Взаимозависимость систем управления безопасностью и качеством услуг безопасности является обязательным морфологическим признаком общей организационной структуры СЗИ. Так, любой существенный сбой в работе СЗИ приводит к снижению гарантий в предоставлении нужных услуг, что неизбежно скажется на уровне безопасности. В тоже время ошибки персонала также способны снизить уровень безопасности. Поэтому возникает необходимость в исследовании процессов управления безопасностью и качеством услуг, которые создаются и функционируют в рамках как отечественных нормативных документов, так и международных стандартов, а также процессов взаимодействия между ними [4, 5].

Можно выделить фундаментальный признак общности между стандартами и нормативными документами, если учесть что

$$\boldsymbol{ND} \cap \boldsymbol{ISO} = \boldsymbol{SM} \tag{1}$$

где ***ND*** – нормативные документы по защите информации в автоматизированных системах, ***ISO*** – «Основные критерии», ***SM*** – общность стандартов, определенная через понятие «система управления».

Системы управления вида (1) создаются в рамках организационной структуры СЗИ как средство, обеспечивающее проведение определенной политики в достижении поставленных целей в области защиты информации, локализованных требованиями по обеспечению безопасности в автоматизированных системах (АС) передачи информации. Поэтому системное исследование должно быть основой как при построении, так и при эксплуатации СЗИ с заданным качеством услуг [6].

III Основная часть

Общность подхода к управляемой системе в рамках целенаправленного действия дает право рассматривать ее как отображение $\sum$, построенное на объединении двух функций: внешней и внутренней. Такое объединение следует определить как некоторое согласованное множество, полученное в результате следующей операции:

$$\sum : \boldsymbol{F}_1 \text{ Y } \boldsymbol{F}_2 \to \boldsymbol{L} \tag{2}$$

где $[F_1] \subset \boldsymbol{F}_1$; $[F_2] \subset \boldsymbol{F}_2$, а $\boldsymbol{L}$ – целенаправленное действие в управляемой системе, отвечающее условиям, закрепленным во внешней и внутренней функциях.

В согласованном множестве (2) принято, что внешняя функция $\boldsymbol{F}_1$ является преобладающей и служит причиной, формирующей внутреннюю функцию $\boldsymbol{F}_2$ управляемой системы, т. е.

$$\boldsymbol{F}_1 \to \boldsymbol{F}_2 \,. \tag{3}$$

В технических и организационных системах управления СЗИ связь между причиной и следствием вида (2) всегда имеет место. Именно внешняя функция способна дать представление о внутренней структуре системы, а также возможность оценить качество управления. Для этого необходимо чтобы внешняя функция была определена в классе рекурсивно-вычислимых функций [4]. При заданной внешней и подобранной внутренней функциях имеется возможность получить представление о структуре управляемой системы и ввести ограничения на внутреннюю функцию $\boldsymbol{F}_2$. Так, ограничения, накладываемые на структуру внутренней функции управляемой системы, способны решить проблему размерности или алгебраической сложности, а также проблемы идентификации. Метод конструирования системы управления в виде отображения (2) позволяет сделать прозрачной процедуру составления малопараметрических математических моделей управляемых СЗИ [4]. Поэтому особенностью, которую необходимо учитывать при построении системы управления, является приоритет внешней функции $\boldsymbol{F}_1$ над внутренней $\boldsymbol{F}_2$.

Введенные функции $\boldsymbol{F}_1$ и $\boldsymbol{F}_2$ имеют абстрактный характер, так как отвечают только на два общих вопроса, касающихся управляемой СЗИ – зачем система создается или выделяется и каким образом в системе получается желаемый результат. Объединение ответов, сформулированное с помощью $\boldsymbol{F}_1$ и $\boldsymbol{F}_2$, раскрывает одно общее свойство системы – целенаправленное действие, происходящее в ней самой и с ее элементами. Действие должно быть организовано так, чтобы оно позволяло реализовать поставленную цель, конкретизированную с помощью $\boldsymbol{F}_1$. Следовательно, отображение объединения внутренней функции $\boldsymbol{F}_2$ и внешней $\boldsymbol{F}_1$ можно рассматривать как целенаправленное действие $\boldsymbol{L}$, способное полностью описать управляемую систему. Замкнутость внешней и внутренней функций естественным образом порождает замкнутость целенаправленного действия, так что $[L] \subset \boldsymbol{L}$.

Поэтому в любых системах управления, в частности, СЗИ, можно охарактеризовать такое действие

следующим замкнутым по объединению выражением

$$\boldsymbol{L} = \boldsymbol{SS} \text{ Y } \boldsymbol{TQ} \text{ Y } \boldsymbol{SA}, \tag{4}$$

где $\boldsymbol{SS}$ – непустое связанное и замкнутое множество элементов, составляющих систему; $\boldsymbol{TQ}$ – общая характеристика целенаправленного действия между элементами; $\boldsymbol{SA}$ – самооценка результатов движения системы к цели управления $\boldsymbol{F}_1$.

Исходя из определения управляемой системы вида (2) как целенаправленного действия (4), можно рассматривать структуру СЗИ лишь как представление (4), допускающее снижение уровня абстрагирования $\boldsymbol{L}$, заложенного с помощью функций $\boldsymbol{F}_1$ и $\boldsymbol{F}_2$. Для снижения уровня абстрагирования целенаправленного действия следует привлекать такие аспекты этого действия, как его геометрические, кинематические, механические, физические, морфологические свойства [3]. Причем в системах управления вида (4) понизить уровень абстрагирования можно, если использовать, например, только морфологические аспекты, как более общие по отношению к остальным. Морфологическим свойством целенаправленного действия $\boldsymbol{L}$ в (2) будем называть некоторое множество физических свойств, которые способны порождать функциональные отношения между отдельными элементами системы. Именно такая взаимосвязь между функцией и структурой позволяет осуществить операцию декомпозиции целенаправленного действия $\boldsymbol{L}$ в системе (2) по конечномерному базису морфологических свойств [3].

Очевидно, что морфологическим классом функций целенаправленного действия $\boldsymbol{L}$ в системе следует считать их множество, которое связано, по крайней мере, одним общим морфологическим свойством. Тогда $\boldsymbol{L}$ можно представить как класс с характеристикой, определенной на уровне соотношения эквивалентности вида:

$$\boldsymbol{A} \subset \boldsymbol{L} \times \boldsymbol{L},$$

а упорядоченная пара $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ образует систему с отношением, описывающую этот класс, для которого $\boldsymbol{A}$ является показателем неразличимости целенаправленных действий. Следовательно, понятие управляемой системы (2) как объединение внешней и внутренней функции в силу замкнутости (4) можно сопоставить и приравнять к понятию оператора, который определен в классе $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ и образует внутреннюю функцию системы, а внутреннее целенаправленное действие (2) необходимо рассматривать только с морфологических позиций, так как изменения, касающиеся характера оператора, не влияют на сущность этого действия [4].

В зависимости от внешней функции, формирующей систему, морфология класса $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ может быть декомпозирована как в узком, так и в широком смысле. Уровень декомпозиции оператора из $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ способен объяснить такое важное понятие, как внутренний масштаб системы. Определение оператора системы (2) с помощью внешней и внутренней функции, ограничение (3) и фиксация его в классе $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ позволяют считать, что в данном случае целенаправленное действие полностью определено, а, следовательно, морфологические свойства, формирующие такой класс эквивалентности, поддаются обязательной декомпозиции. Процесс декомпозиции неизбежно приведет к представлению $\boldsymbol{L}$ из $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$ как полного класса непересекающихся морфологических свойств целенаправленного действия [4]. Здесь следует заметить, что всякое морфологическое действие сводится к такому же множеству физических действий. Помимо этого, способ задания оператора классом $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$, по своей сути, равноценен определению физического объекта.

Введенный класс эквивалентности целенаправленного действия и его декомпозиция по морфологическим свойствам позволяют исследовать тонкую структуру оператора, но лишь в рамках его локализации. Однако требование замкнутости оператора выполнимо лишь при констатации сведений о самом замыкании. Именно замыкание фиксирует внешние условия, по отношению к которым протекает само действие, обеспечивая как реализацию цели $\boldsymbol{F}_1$, так и необходимую внутреннюю практическую деятельность. Поэтому при синтезе системы управления защитой информации в АС появляется необходимость в расширении морфологического класса целенаправленных действий вида $<\boldsymbol{L}, \boldsymbol{A}>$ за счет дополнительного включения в него геометрических, кинематических, механических, физических и морфологических аспектов замыкания такого действия [6]. Расширенный за счет включения свойств замыкания морфологический класс оператора уже определяет не только тонкую структуру целенаправленного действия, являющегося элементом этого класса, но дает и общее глобальное представление о деятельности СЗИ и ее движении к поставленной цели в пределах структурных

представлений о замыкании. Такой обобщенный класс целенаправленных действий можно назвать структурным классом эквивалентности системы. Следует отметить, что, в тех случаях, когда структура замыканий $\boldsymbol{F}_1$ и $\boldsymbol{F}_2$ определена только на уровне морфологических свойств, структурный класс вырождается в морфологический [4].

Если принять во внимание, что множество действий $[L_0] \subset \boldsymbol{L}_0$, включающее в себя и морфологические свойства замыкания, обладает отношением эквивалентности $\boldsymbol{R} = \boldsymbol{L}_0 \times \boldsymbol{L}_0$, то упорядоченная пара $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$ будет характеризовать общее пространство приближений для $\boldsymbol{L}_0$. Тогда упорядоченная пара $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{R}>$ представляет собой систему с отношением, которая так же, как и $<\boldsymbol{L}_0, \boldsymbol{A}>$, является характеристикой пространства приближений и допускает декомпозицию по классам эквивалентности, организованным, например, на основе морфологических или более тонких физических свойств целенаправленного действия. Такие классы следует рассматривать, как элементарные множества в $\boldsymbol{\Psi}$, а всякое их объединение приводит к образованию составного множества в $\boldsymbol{\Psi}$, принятого за общее пространство приближений для $\boldsymbol{L}_0$, причем всегда выполняется условие:

$$\boldsymbol{L} \subset \boldsymbol{L}_0.$$

Задача декомпозиции класса $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$, так же как и его подкласса $\boldsymbol{\Psi} = <\boldsymbol{L}, \boldsymbol{A}>$, решаема лишь в том случае, когда действие, замкнутое, например, по объединению (4), допускает выделение морфологических свойств, являющихся более тонкими по отношению к составляющим (4). В силу определения морфологических свойств объекта или явления, их можно идентифицировать лишь тогда, когда они определяют физические признаки, обладающие нижней и верхней границами. Детализация морфологических свойств структурного класса $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$ и их аксиоматизация порождают понятие модели [4].

Свойства структурного класса $<\boldsymbol{L}_0, \boldsymbol{R}>$ преобразуются в теорию модели управляемой системы (систему аксиом) лишь в случае непротиворечивости самих аксиом. Обычно для достаточно широкого класса формальных теорий условие непротиворечивости группы аксиом $\boldsymbol{G}$ равносильно существованию в их общности хотя бы одного недоказуемого предложения. Поэтому свойство непротиворечивости в аксиоматической группе $\boldsymbol{G}$ следует рассматривать как необходимое для существования самих моделей. Однако такая необходимость способна дать описанию действия конкретность и гарантировать его только на уровне общего характера процесса, идущего в моделях класса $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$, и неспособна в полной мере обеспечить условие достаточности. Достаточность может возникнуть на непротиворечивой аксиоматической группе класса эквивалентности лишь в тех случаях, когда пространство приближений $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$ замкнуто.

Общность внешней функции $\boldsymbol{F}_1$ для всех элементов из $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$ и локализация целенаправленного действия позволяют принять, что непротиворечивость аксиоматической группы морфологических свойств этого действия способны породить в $\boldsymbol{G}$ не только необходимость, но и достаточность. Тогда условия необходимости и достаточности превращают группу $\boldsymbol{G}$ в теорию, т. е.

$$<\boldsymbol{L}_0, \boldsymbol{R}> \rightarrow \boldsymbol{T},$$

где $\boldsymbol{T}$ – теория систем управления защитой информации, определяющая пространство приближений $\boldsymbol{\Psi}$.

Не менее важным свойством для практического использования теории модели управляемой системы является ее полнота [3]. Полнота аксиоматизированных морфологических свойств группы $\boldsymbol{G}$ позволяет в рамках этой теории считать верными все рассматриваемые процессы функционирования системы, выводимые из теории $\boldsymbol{T}$ для пространства приближений $\boldsymbol{\Psi}$. Теорию пространства приближений можно считать полной, если для непустого класса $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$ любое действие, следующее из процесса функционирования системы, является истинным в каждой отдельной модели. Полнота класса $\boldsymbol{\Psi}$ обеспечивает достижение цели управления, и в этом смысле она должна признаваться позитивной.

IV Выводы

Анализ структуры $\boldsymbol{\Psi} = <\boldsymbol{L}_0, \boldsymbol{R}>$, выполненный путем декомпозиций по отдельным морфологическим свойствам, позволил получить конечномерное пространство приближений с базисом в виде аксиоматизированной группы суждений, обращающих теорию модели и формирующих класс, который

можно записать как

$$\boldsymbol{M} \sim mod\ \boldsymbol{T}.$$

Тогда при решении практических задач приведенное выше соотношение дает право учитывать в процессе составления нормативных документов по управлению обеспечения защитой информации в АС описание свойств класса ***M.***

Литература: ***1****. Расстригин Л. А. Адаптация сложных систем. Методы и приложения. – Рига: Зинатне, 1981. – 375 с.* ***2****. Общие критерии оценки безопасности информационных технологий: Уч. пособие. Пер. с англ. Е. А. Сидак / Под ред М. Т. Кобзаря. – М.: МГУЛ, 2001. – 81 с.* ***3****. Зубов В. И. Лекции по теории управления. М.: МГУ, 1975. –496 с.* ***4****. Романов О. І., Лівенцев С. П., Павлов І. М. Математична модель захисту інформації в автоматизованих мережах спеціального призначення // Збірник наукових праць ВІТІ НТУУ „КПІ”. – К.: ВІТІ НТУУ „КПІ”. – 2004. – Вип. 5. – С. 147-153.* ***5.*** *Подиновский В. В. Количественная важность критериев // Автоматика и телемеханіка. – 2000. – №5. – С. 110-123.* ***6****. Кононович В. Г., Голобородько Д. В. Методи та засоби захисту від несанкціонованого доступу в системі управління мережами електрозв'язку України // – К.: Зв'язок, № 2, 1999, с. 13-16.*

УДК 681.3:519.872

ПОСТАНОВКА ЗАДАЧИ ОПТИМАЛЬНОГО ВЫБОРА ФУНКЦИОНАЛЬНОГО ПРОФИЛЯ ЗАЩИЩЕННОСТИ

Анатолий Антонюк, Денис Берестов*, Сергей Пустовит*, Владимир Шилин**
Национальная академия государственной налоговой службы Украины
**ННДЦ оборонных технологий и военной безопасности Украины*
***Институт программных систем НАНУ*

Аннотация: **Рассмотрена постановка формальной задачи выбора оптимального профиля защищенности в автоматизированных системах. Детально описаны основные характеристики задачи.**
Summary: **The formal task to choice optimal profile of security in computer systems are considered. In details the common characteristics of the task are described.**
Ключевые слова: **Информационная система, защита информации, угроза, модель, ущерб, вероятность.**

I Введение

Как известно [1 – 4], процесс создания любой системы защиты информации (СЗИ) в защищенных автоматизированных системах (АС) включает обязательную процедуру выбора и последующей реализации стандартного функционального профиля защищенности (СФПЗ). В [3] приводится классификация АС и список из 90 СФПЗ. Таким образом, в задачу разработчика входит обследование свойств конкретной АС, как объекта защиты и выбор необходимого СФПЗ из данного списка. Там же отмечено, что в случае, когда ни один СФПЗ из данного списка не подходит к конкретной АС, разработчик должен создать свой, наиболее подходящий для него СФПЗ, обосновать и утвердить его.

В [5] предложен подход к решению этой проблемы, который базируется на формализованном описании свойств АС и свойств СФПЗ и дальнейшем использовании взаимно однозначной зависимости между этими свойствами. Для установления этой зависимости используется уже известный список СФПЗ, что и позволяет определять наиболее подходящий СФПЗ для данной АС. Однако не всегда удается четко формализовать свойства АС и установить связь между ними и необходимым СФПЗ.

В [6] предложена формальная постановка задачи синтеза оптимальной СЗИ, позволяющая определять наиболее рациональный вариант технической реализации СЗИ. Данный поход может быть использован для формулировки задачи выбора оптимального СФПЗ.

Напомним, что согласно нормативным документам [1 – 4] каждый СФПЗ является набором соответствующих функциональных услуг. Каждая услуга является набором функций, позволяющих противостоять определенному множеству угроз, причем каждая услуга может включать несколько уровней. Чем выше уровень услуги, тем более полно обеспечивается защита от определенного вида угроз. Уровни услуг имеют иерархию по полноте защиты, хотя и не являются точными подмножествами друг