УДК 681.3.06

А.В. ПОТИЙ, д-р техн. наук, Д.Ю. ПИЛИПЕНКО

МОДЕЛЬ ИНСТИТУЦИОНАЛЬНОГО УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Введение

Сегодня можно с уверенностью утверждать, что понимание проблем управления процессами защиты информации (ЗИ) подвергается качественному изменению. Работающие в данном направлении исследователи отмечают важность организационных (нетехнических аспектов) защиты информации наравне с техническими [1 – 3]. С точки зрения управления и оценки, организационные аспекты ЗИ (человеческий фактор, культура информационной безопасности) представляют собой значительную сложность. Одновременно с этим присутствует острая потребность в разработке моделей управления деятельностью по ЗИ, которые учитывают организационные аспекты ЗИ.

Исследование деятельности по ЗИ осуществляется в рамках новых теоретических моделей и подходов. К таким моделям и подходам относятся: процессный подход, игровая модель ЗИ, программно-целевой подход, сценарный подход, рациональная модель ЗИ, ситуационный подход, институциональное управление. Модель институционального управления деятельностью по ЗИ в рамках исследования организационных аспектов представляет значительный интерес.

В работе приводятся результаты онтологического моделирования института информационной безопасности (ИИБ) и предметной области культуры информационной безопасности (КИБ). Предлагается модель институционального управления деятельностью по ЗИ. Формулируются выводы и рекомендации относительно применения институционального подхода в деятельности по ЗИ.

1. Предметная область института и культуры информационной безопасности

Ключевой функцией ИИБ является согласование целей деловой деятельности организации с задачами безопасности и профессиональными обязанностями персонала. На рис. 1 приведена онтологическая модель терминологического ядра предметной области ИИБ, раскрывающая взаимосвязь между основными понятиями (компонентами).

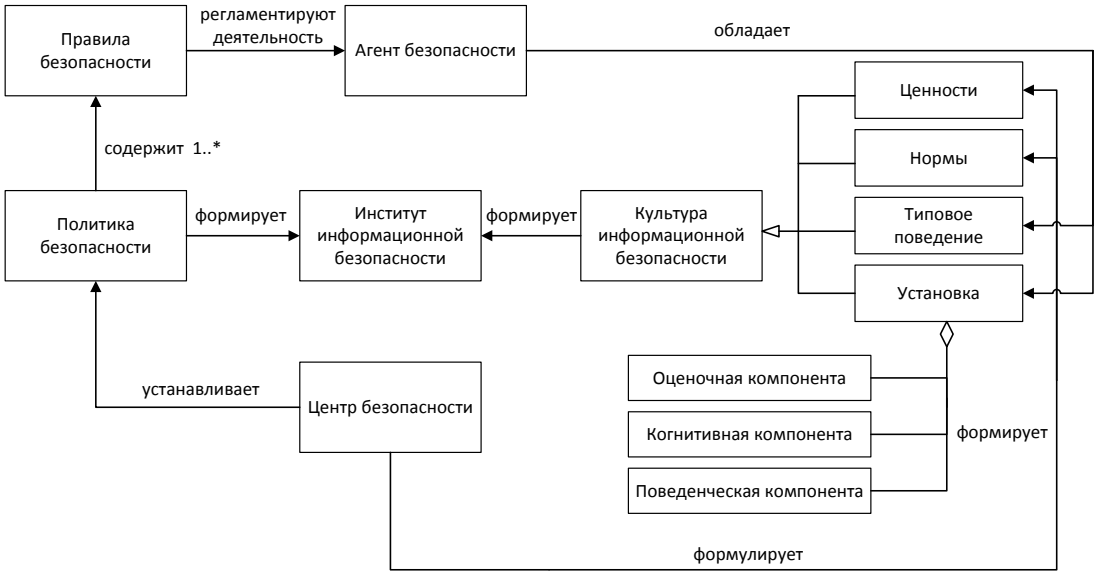

Рис. 1. Онтологическая модель предметной области института и культуры информационной безопасности

Анализ приведенной модели позволяет предложить следующее определение понятия “институт информационной безопасности”:

Определение 1.1. *Институт информационной безопасности это упорядоченная система ценностей, норм и правил безопасности в контексте защиты информации, формирование которого направлено на согласование деятельности агента безопасности с целями и задачами, установленными центром безопасности.*

Как видно из онтологической модели (рис. 1), на формирование ИИБ оказывают влияние два субъекта деятельности по ЗИ: центр безопасности и агент безопасности. Центр безопасности может быть представлен руководством организации, начальником службы безопасности или другими управляющими субъектами, чьи интересы должны быть защищены. Агент безопасности представлен сотрудником организации или другим лицом, которое не принимает непосредственного участия в процессе формирования управляющих воздействий.

Определение 1.2. *Центр безопасности – это субъект, который осуществляет управление деятельностью по защите информации, проводит целенаправленное формирование политики безопасности и культуры информационной безопасности с конечной целью сформировать институт информационной безопасности.*

Определение 1.3. *Агент безопасности – это управляемый субъект деятельности по защите информации, который оказывает влияние на формирование культуры информационной безопасности посредством своего поведения и установок по отношению к требованиям безопасности.*

Культура информационной безопасности является не только существенным фактором, который оказывает влияние на общую защищенность организации, но и частью более сложной структуры – института информационной безопасности. В рамках модели институционального управления предлагается рассматривать КИБ как инструмент управления деятельностью по ЗИ. Сущность институционального управления заключается в формировании норм и правил безопасности. Нормы и правила могут быть выражены в явной и неявной форме. Тогда политику безопасности можно отнести к группе явных форм, а КИБ отнести к неявной форме выражения норм и правил. Следует подчеркнуть, что в организационном аспекте политика безопасности представляет собой механизм принуждения, в то время как КИБ представляет собой механизм побуждения. Предлагается следующее определение КИБ:

Определение 1.4. *Культура информационной безопасности – это набор норм, ценностей, установок и стандартов, которые формируют допустимое поведение в контексте деятельности по защите информации.*

2. Модель институционального управления безопасностью информации

Модель институционального управления безопасностью информации представлена на рис. 2. Данная модель состоит из четырех блоков: мотивационный аспект, модель центра безопасности, модель агента безопасности, модель оценки уровня КИБ. Субъектами деятельности по ЗИ в данной модели выступают центр безопасности (управляющий субъект) и агент безопасности (управляемый субъект).

2.1. Мотивационный аспект деятельности по ЗИ.

Не вызывает сомнений, что в основе любой человеческой деятельности лежит определенная потребность. Наличие потребности формирует у субъекта деятельности мотив и цель. В контексте ЗИ потребность проявляется в том, что субъект деятельности по ЗИ ощущает необходимость в обеспечении такого состояния информации, при котором не существует угроз информационным активам организации или же их уровень приемлем. Цель отражает желаемый результат, достижение которого способно удовлетворить потребностям субъекта деятельности по ЗИ. Мотив выступает побудителем к действию, являясь тем, ради чего осуществляется деятельность по ЗИ.

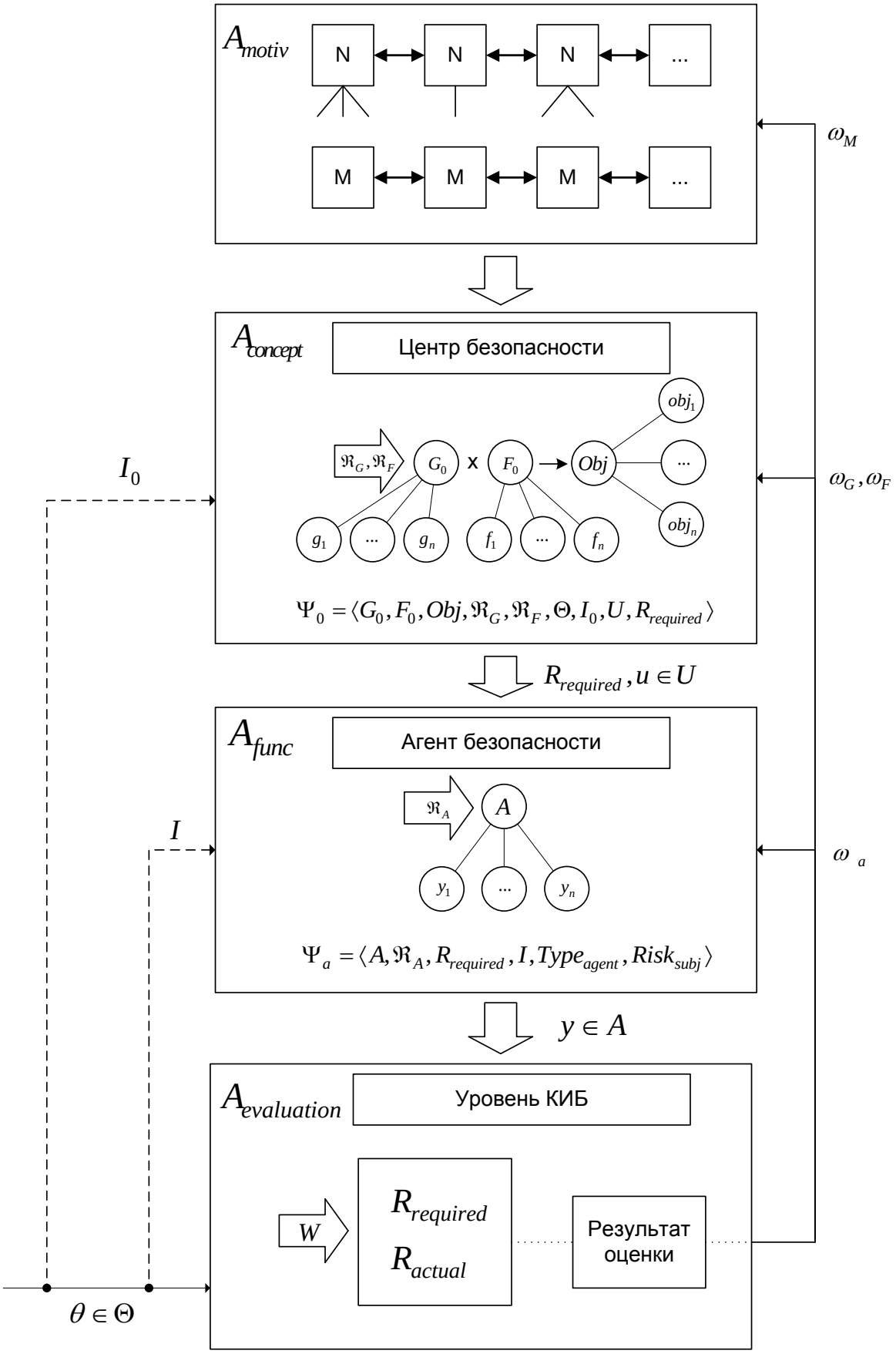

Рис. 2. Модель институционального управления деятельностью по ЗИ

Центр обладает рядом потребностей и, как следствие, совокупностью мотивов. Как видно из блока A_{motiv} (рис. 2), количество связей между потребностью и мотивом может варьироваться. Это зависит как от специфики организации, в которой находится субъект деятельности по ЗИ, так и от индивидуальных особенностей его как личности. Наличие множества потребностей N и множества мотивов M приводит к формированию концепции обеспечения безопасности информации (блок $A_{concept}$).

2.2. Модель центра безопасности

Деятельность центра безопасности заключается в реализации некоторого управляющего воздействия $u(\cdot) \in U$ по отношению к агенту. Как видно из рис. 2, выбор стратегии $u(\cdot)$ из множества допустимых стратегий U является результирующим этапом процесса принятия решения центром. Принято считать, что центр не производит результат деятельности, не опосредованный агентом. Роль центра заключается в выборе типа управления и его реализации, поэтому результатом деятельности центра принято считать результат деятельности агента [4]. Выбор управляющего воздействия описывается моделью принятия решений центром безопасности Ψ_0.

Помимо управляющего воздействия $u(\cdot) \in U$, модель принятия решений центра безопасности включает в себя: множество целей ЗИ G_0, множество факторов F_0, функции предпочтений $\Re_G, \Re_F$ на множестве целей и множестве факторов соответственно, множество задач безопасности $Obj = \{obj_1, obj_2, ..., obj_n\}$, множество обстановок Θ, информацию о конкретной обстановке на момент принятия решения I_0, требуемые результаты деятельность по ЗИ. Модель принятия решений центром можно описать следующим кортежем:

$$\Psi_0 = \left\langle G_0, F_0, Obj, \Re_G, \Re_F, \Theta, I_0, U, R_{required} \right\rangle \quad (1)$$

На данном этапе центр формулирует главные цели защиты информации G_0 и в случае необходимости осуществляет их декомпозицию на требуемое число подцелей $g_i \in G$. Расставляя приоритеты между целями, центр использует свои предпочтения на множестве целей $\Re_G$. Пространство целей ЗИ является в достаточной мере гибким, поэтому декомпозиция целей может осуществляться как на этапе проектирования, так и непосредственно в ходе осуществления деятельности по ЗИ. Достижение целей ЗИ g_i происходит под влиянием множества факторов F_0. Аналогично множеству целей, множество факторов также подвергается декомпозиции. Центр осуществляет ситуационный анализ и выделяет наиболее существенные факторы, опираясь на свои предпочтения на множестве факторов $\Re_F$. Соотношение целей $g_i \in G$ и факторов $f_i \in F$ формирует множество задач защиты информации $Obj = \{obj_1, obj_2, ..., obj_n\}$. Решение задач ЗИ является механизмом осуществления деятельности по ЗИ посредством выполнения конкретных действий (набора операций).

Таким образом, опираясь на множество задач безопасности $Obj = \{obj_1, obj_2, ..., obj_n\}$, центр безопасности может сформулировать требуемый результат $R_{required}$.

Содержательно в данной модели требуемый результат $R_{required}$ будем понимать как уровень культуры информационной безопасности, которая формируется на основе поведения агентов, являющихся результатом управляющих воздействий центра безопасности.

Отклонение фактического результата R_{actual} от требуемого $R_{required}$ может быть обусловлено влиянием обстановки на действия агента: реализацией внешних или внутренних угроз, системными сбоями, действиями других субъектов системы ЗИ и т.д. Данная зависи-

мость выражается функцией $r = W_I(\cdot) = (y, \theta)$, где $r \in R_{actual}$ фактический результат деятельности агента, $y \in A$ действие агента, и $\theta \in \Theta$ частная обстановка на момент действия. Информация, доступная центру о частной обстановке, определяется переменной I_0.

Таким образом, результатом работы модели принятия решений Ψ_0 является некоторое управляющее воздействие $u(\cdot)$. В общем виде задача центра заключается в выборе оптимального воздействия $u(\cdot)$ из множества допустимых альтернатив $u(\cdot) \in U$. В зависимости от своих предпочтений, ограничений на ресурсы и возможностей центр выбирает наиболее рациональное управляющее воздействие на момент принятия решения.

2.3. Модель принятия решений агентом безопасности.

Как уже упоминалось, агент безопасности играет роль управляемого субъекта деятельности по ЗИ. Для того чтобы лучше понять принцип выбора агентом тех или иных действий, необходимо описать модель принятия решений агентом (блок A_{func}). В общем виде данная модель описывается кортежем вида:

$$\Psi_a = \left\langle A, \Re_A, R_{required}, w(\cdot), I, Type_{agent}, Risk_{subj} \right\rangle. \quad (2)$$

Пусть агент безопасности обладает предпочтениями $\Re_A$ на множестве действий A и способен выбирать действие $y \in A$. В зависимости от своего типа $Type_{agent}$ и степени субъективного восприятия риска $Risk_{subj}$, агент склоняется к выбору тех или иных действий. Содержательно тип агента $Type_{agent}$ можно интерпретировать как его манеру взаимодействия с центром: благожелательность, нейтральность или противодействие. Переменная $Risk_{subj}$ выступает мерой субъективного восприятия риска агентом лично. Например, агент с низким уровнем восприятия риска может проигнорировать принятые в организации правила (политику) и нормы безопасности в том случае, когда негативные последствия для него лично не имеют существенного значения.

При выборе действия $y \in A$ агент руководствуется собственными предпочтениями на множестве действий A. Функция $W_I(\cdot)$ устанавливает зависимость между выбором действия $y \in A$, обстановкой $\theta \in \Theta$ и результатом деятельности по ЗИ $r \in R_{actual}$. Тогда выбор действия агента определяется правилом индивидуального рационального выбора:

$$P^{W_I}(Type_{agent}, Risk_{subj}, I, A) \subseteq A \quad (3)$$

Как видно из выражения (3), на выбор агентом безопасности действия $y \in A$ влияет тип агента $Type_{agent}$, мера его субъективного восприятия риска $Risk_{subj}$, информация об обстановке на момент принятия решения I, множество допустимых действий A. Пользуясь данным правилом, из всего множества допустимых действий A агент формирует подмножество наиболее предпочтительных с его точки зрения действий $\tilde{A} \in A$.

Описания поведения агента безопасности будем осуществлять в рамках следующих гипотез [4]: *гипотезу рационального поведения агента* и *гипотезу детерминизма*. Первая гипотеза заключается в том, что агент на основе всей имеющейся у него информации выберет действие, ведущее к наиболее предпочтительным для него результатам. Вторая гипотеза означает стремление агента устранить существующую неопределенность и принимать решения в условиях полной информированности.

2.3.1. Гипотеза рационального поведения агента безопасности.

Согласно гипотезе рационального поведения агент выбирает решение из множества альтернатив, на которых достигается максимум его функции полезности:

$$f(y) = v(w(y, \theta)) \tag{4}$$

Следует отметить, что между действием агента $y \in A$ и результатом $r \in R_{actual}$ не существует *однозначной* связи. Это объясняется тем, что помимо поведения агента, на формирование КИБ также влияет обстановка, которая не всегда связана с действиями агента. Принимая решение, агент стремится прогнозировать результаты своей деятельности с учетом информации, которая отражена в переменной I. Например, на соблюдение требований безопасности работника бухгалтерии повлияет его знание о том, проводится ли систематический контроль его действий. Знание о мониторинге электронной почты может предотвратить нарушение требований безопасности другим агентом. Подобная информированность неизменно отразится на решении, принимаемом агентом безопасности.

С целью осуществить наиболее эффективное действие, максимизирующее функцию полезности, агент стремится устранить неопределенность. Неопределенность, в зависимости от направленности на объекты или субъекты, может быть объективной или субъективной соответственно. Объективная неопределенность касается параметров обстановки, т.е. условий, которые агент учитывает при принятии решения. Данная неопределенность устраняется увеличением информированности агента с помощью параметра I. Например, доведение до сведения сотрудника правил работы с электронной почтой. Субъективная неопределенность представляет собой неполную информированность агента о принципах поведения других субъектов. Уменьшить данную неопределенность способен центр при помощи *рефлексивного управления*, т.е. предоставляя агентам информацию о параметрах других участников системы ЗИ. Например, сотрудники информируются о нарушениях безопасности, произошедших по вине их коллег.

2.3.2. Гипотеза детерминизма.

В случае детерминированного изменения результата деятельности информация об обстановке является несущественной для агента, поскольку в данном случае результат зависит только от действия агента. Иными словами, каждому действию агента соответствует только один результат деятельности $f(y) = v(w(y))$. Правило индивидуального рационального выбора в данном случае будет выглядеть следующим образом:

$$P^{W_I} = (Type_{agent}, Risk_{subj}, A) = Arg \max_{y \in A} f(y) \tag{5}$$

Можно сказать, что в таких обстоятельствах существующая неопределенность устранена, и агент безопасности принимает решение в условиях полной информированности. В этом случае влияние внешней природы на формирование КИБ, и оказать влияние на ее текущее состояние может только агент своим поведением.

Гипотеза детерминизма на практике практически нереализуема, поэтому центр безопасности принимает все управляющие воздействия в предположении о рациональности поведения агента безопасности.

2.4. Модель оценки уровня культуры информационной безопасности.

Для оценки уровня КИБ необходимо задать множество качественных или количественных показателей. При формировании множества показателей безопасности должны быть учтены цели безопасности G_0, факторы F_0 и задачи безопасности $Obj = \{obj_1, obj_2, ..., obj_n\}$ (модель $A_{concept}$). Для описания соответствия реального результата деятельности по ЗИ

требуемому результату $R_{required}$ введем числовую функцию соответствия на множестве результатов:

$$\rho = \rho(Y(u), R_{required}) \tag{6}$$

Фактический результат деятельность по ЗИ $Y(u) \in R_{actual}$ может быть получен как результат оценки уровня КИБ на основе множества показателей безопасности информации W. Таким образом, возникает задача разработки системы показателей безопасности, на основе которой может получен интегральный показатель $\tilde{W}$. Модель оценки уровня КИБ в общем виде представляется следующим кортежем:

$$A_{eval} = \left\langle \rho, Y(u), R_{required}, W \right\rangle \tag{7}$$

На основе полученных результатов оценки центр безопасности в случае необходимости вносит корректировки $\omega_M, \omega_G, \omega_F, \omega_a$ на необходимом уровне институционального управления деятельностью по ЗИ. Переменная ω_M отражает изменение множества мотивов центра безопасности, ω_G и ω_F отражает изменение множества целей и факторов соответственно, ω_a означает корректировки, касающиеся управляющего воздействия, направленного на агента безопасности.

Выводы

Институциональное управление деятельностью по защите информации сегодня является перспективным подходом к решению проблем управления организационными аспектами деятельности по ЗИ. Природа данного типа управления позволяет осуществлять управление как явными, так и неявными формами норм и правил безопасности, которые накладывают ограничения на деятельность сотрудников организации или мотивирует их к соблюдению политики безопасности.

Предложенная модель управления раскрывает природу поведения агента безопасности, позволяя центру безопасности вырабатывать управленческие решения с учетом гипотезы рациональности агента безопасности. Установлено, что поведение агента зависит от его типа, меры субъективного восприятия риска и правила индивидуального выбора, которым руководствуется агент безопасности.

Активными компонентами данной модели выступают центр безопасности и агент безопасности. Поведение агента безопасности, как было показано, оказывает значительное влияние на формирование КИБ. В то же время центр безопасности, как управляющий субъект, должен формировать поведение агента, учитывая его параметры в ходе осуществления необходимых управляющих воздействий.

В качестве направления дальнейших исследований представляется актуальной разработка метода численной оценки уровня КИБ, разработка множества показателей безопасности для оценки уровня КИБ и их классификация, формализация процедуры оценивания.

Список литературы: 1. *Dhillon, G. and Torkzadeh, G.* Value-focused assessment of information system security in organizations // Information Systems Journal. 2006. 16:293-314. 2. *Siponen, M.,* Oinas-Kukkonen, H.07). A review of information security issues and respective research contributions // SIGMIS Database. 2007. 38(1):60-80. 3. *Vroom, C., von Solms, R.* Towards information security behavioral compliance // Computers & Security. 2004. 23(3):191-198. 4. *Новиков, Д.А.* Институциональное управление организационными системами. – М. : ИПУ РАН, 2004. – 68 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 14.09.2012