УДК 681.3.06

А.В. Потий[1], Д.Ю. Пилипенко[2], Д.В. Кепко[3]

[1] *Харьковский национальный университет имени В.Н. Каразина, Харьков*
[2] *Харьковский национальный университет радиоэлектроники, Харьков*
[3] *Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков*

МОДЕЛЬ ИНСТИТУЦИОНАЛЬНОГО УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В данной статье предлагается обобщенная модель институционального управления информационной безопасностью, и рассматриваются ее ключевые компоненты: мотивационный, концептуальный, функциональный и оценочный. Также рассмотрены основные субъекты деятельности по обеспечению безопасности информации и их взаимосвязь с компонентами модели.

***Ключевые слова**: институциональное управление, центр безопасности, агент безопасности.*

Введение

Сегодня можно с уверенностью утверждать, что понимание проблем управления процессами защиты информации (ЗИ) подвергается качественному изменению. Работающими в данном направлении исследователями все чаще отмечается важность учета нетехнических аспектов деятельности по обеспечению безопасности информации наравне с техническими (ОБИ) [1 – 3]. Человеческий фактор, культура безопасности и организационные нормы обеспечения безопасности представляют определенную сложность с точки зрения управления и учета в виду их неколичественной природы. Одновременно с этим присутствует острая потребность в разработке формализованных моделей управления деятельностью по ОБИ, которые учитывают упомянутые выше нетехнические аспекты ЗИ. Таким образом, определенную актуальность представляет модель институционального управления деятельность по ОБИ как предмет исследования. Концепция институционального управления подразумевает управление нормами и ограничениями, что выглядит перспективным подходом к решению рассмотренных выше проблем. Данная модель призвана учесть нетехнические аспекты деятельности по ОБИ и помочь в осуществлении их контроля.

1. Институт информационной безопасности

Основной функцией института информационной безопасности (ИИБ) является согласование ключевых целей и задач безопасности с повседневными профессиональными обязанностями сотрудников. На рис. 1 представлена онтологическая модель, которая раскрывает взаимосвязь основных понятий, формирующих терминологическое ядро данной предметной области. Предлагается следующее определение данного понятия: *институт информационной безопасности* это упорядоченная, формализованная система ценностей, норм, правил и стандартов поведения, призванная согласовать деятельность агента безопасности с целями и задачами, установленными центром безопасности.

2. Модель институционального управления безопасностью информации

На рис. 2 представлена модель институционального управления безопасностью информации. Данная

Рис. 1. Онтологическая модель процесса формирования ИИБ

модель была получена на основе обобщенной математической модели управления безопасностью информации, предложенной в [4]. Данная модель состоит из четырех компонент или блоков: мотивационного, концептуального, функционального и оценочного.

Субъектами деятельности по ОБИ в данной модели выступают центр безопасности (управляющий субъект) и агент безопасности (управляемый субъект). Центром безопасности может выступать высшее руководство организации, начальник службы безопасности, администратор безопасности и т.д. Агент безопасности это, как правило, рядовой сотрудник или другое лицо, которое является объектом управления.

2.1. Мотивационный аспект

Не вызывает сомнений, что в основе любой человеческой деятельности лежит некоторая потребность. Наличие потребности в свою очередь формирует у субъекта деятельности мотив и цель. В контексте информационной безопасности (ИБ) 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 в свою очередь выступает побудителем к действию, и является тем, ради чего осуществляется деятельность 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 психологических 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. Концепция деятельности по ЗИ и модель принятия решений центром

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

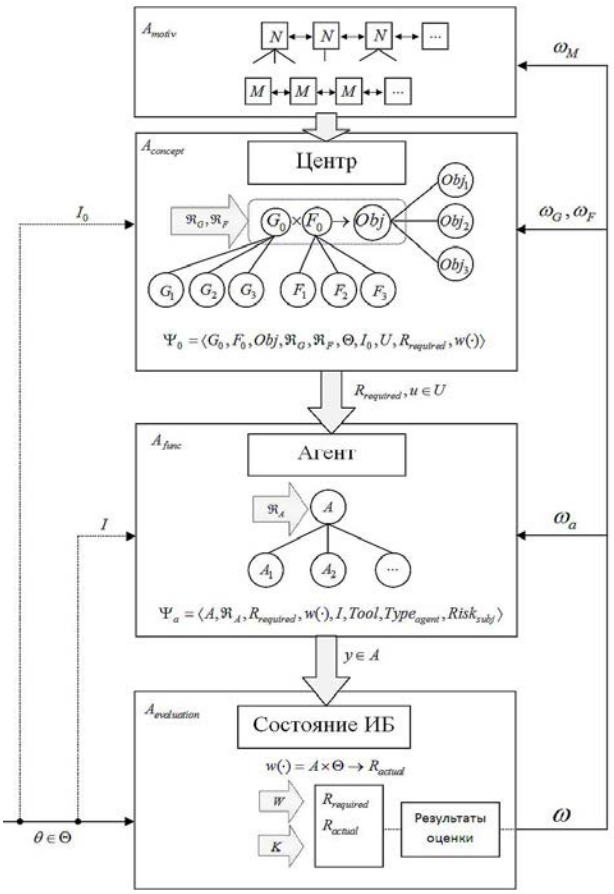

Рис. 2. Модель институционального управления ИБ

Выбор управляющего воздействия описывается моделью принятия решений центра Ψ_0. Помимо управляющего воздействия $u(\bullet) \in U$, модель принятия решений центра включает в себя: множество целей ЗИ G_0, множество факторов F_0, множество задач безопасности $Ob_j = \{Ob_{j1}, Ob_{j2}, ..., Ob_{jn}\}$, функции предпочтений R_G, R_F на множестве целей и множестве факторов соответственно, множество обстановок Θ, информацию о конкретной обстановке I_0 и функцию $w(\bullet)$, которая отражает изменение результата деятельности в зависимости от действия агента и влияния обстановки. В формальном виде модель принятия решений центром можно описать следующим кортежем:

$$\Psi_0 = \left\langle G_0, F_0, Ob_j, R_G, R_F, \Theta, I_0, U, R_{required}, w(\bullet) \right\rangle.$$

На данном этапе центр формулирует главную цель защиты информации G_0 и в случае необходимости осуществляет ее декомпозицию на требуемое число подцелей $g_i \in G$. Расставляя приоритеты между целями, центр использует свои предпочтения на множестве целей R_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, которые могут как способствовать деятельности по ЗИ, так и препятствовать.

Аналогично множеству целей, множество факторов также подвергается декомпозиции. Центр осуществляет ситуационный анализ и выделяет наиболее существенные факторы, опираясь на свои предпочтения на множестве факторов R_F. Соотношение каждой цели $g_i \in G$ и факторов $f_i \in F$ формирует множество задач защиты информации $Ob_j = \{Ob_{j1}, Ob_{j2}, ..., Ob_{jn}\}$. Решение данных задач защиты информации является, по сути, механизмом осуществления деятельности по ЗИ посредством выполнения конкретных действий (набора операций).

Таким образом, сформулировав множество задач безопасности $Ob_j = \{Ob_{j1}, Ob_{j2}, ..., Ob_{jn}\}$, центр может сформулировать требуемый результат $R_{required}$, т.е. результат, который требуется от агента. $R_{required}$ является информацией, которая будет доведена до сведения агента, и представляет собой те результаты, которые нужны центру.

Отклонение фактического результата R_{actual} от требуемого может быть обусловлено влиянием обстановки на действия агента: реализацией внешних или внутренних угроз, системными сбоями, действиями других участников организационной системы и т.д. Данная зависимость выражается функцией $r = w(\bullet) = (y, \Theta)$, 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 $u(\bullet)$. В общем виде задача центра заключается в выборе оптимального воздействия $u(\bullet)$ из множества допустимых стратегий $u(\bullet) \in U$. В зависимости от своих предпочтений, ограничений на ресурсы и возможностей центр выбирает наиболее рациональное управляющее воздействие на данный момент. Помимо институционального управления $u_A \in U_A$, центр может использовать следующие типы управления: мотивационное $u_\nu \in U_\nu$, информационное $u_I \in U_I$, а также любые их комбинации. В случае одновременного использования всех трех типов управления формируется вектор управления вида $U = (U_A, U_\nu, U_I) \in U = U_A \times U_\nu \times U_I$. Более подробно данные типы управления рассмотрены в пункте 3.

2.3. Модель принятия решений агентом

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

$$\Psi_a = \langle A, R_A, R_{required}, w(\bullet), I, Tool, Type_{agent}, Risk_{subj} \rangle .$$

Пусть агент обладает некоторыми предпочтениями R_A на множестве действий A и способен выбирать действие $y \in A$. Предположим, что агент на множестве результатов $R_{required}$ обладает предпочтениями и склоняется к тем или иным действиям в зависимости от своего типа $Type_{agent}$ и степени субъективного восприятия риска $Risk_{subj}$. Множество средств, которыми пользуется агент в ходе осуществления деятельности по защите информации, представлено переменной $Tool$.

Содержательно тип агента $Type_{agent}$ можно интерпретировать как его манеру взаимодействия с центром: благожелательность, нейтральность или противодействие. Личное восприятие риска агента $Risk_{subj}$ оценивает степень субъективного восприятия риска агентом лично. К примеру, агент с низким восприятием риска может проигнорировать правила и нормы безопасности, принятые в организации, когда негативные последствия для него лично не имеют существенного значения. При выборе действия агент руководствуется собственными предпочтениями и некоторым представлением о том, как данное действие способно повлиять на состояние безопасности информации в организации. Как уже упоминалось, данная зависимость описывается некоторым законом $w_I(\bullet)$ изменения состояния безопасности от действия $y \in A$ и обстановки $\theta \in \Theta$. Выбор действия агента определяется правилом индивидуального рационального выбора:

$$P^{W_I} \langle A, I, Type_{agent}, Risk_{subj} \rangle \subset A .$$

Пользуясь данным правилом, из всего множества допустимых действий агент формирует подмножество наиболее предпочтительных действий с его точки зрения. Примем следующие гипотезы: *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

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

$$f(y) = v(w(y,\theta)).$$

Следует отметить, что между действием агента $y \in A$ и результатом $r \in R_{actual}$ не существует *однозначной* связи. Это объясняется тем, что помимо непосредственно поведения агента, на состояние безопасности $r \in R_{actual}$ также влияет обстановка, которая не всегда зависит от действий агента. Таким образом, принимая решение агент учитывает в том числе и влияние обстановки, т.е. прогнозировать результаты своей деятельности с учетом информации об обстановке I. Для того чтобы 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 принимая решение. Данная неопределенность устраняется увеличением информированности агента с помощью параметра I. 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 организационной системы.

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:

$$P^{W_I}\left\langle A, Type_{agent}, Risk_{subj}\right\rangle = \underset{y\in A}{Arg\max}\, f(y).$$

Можно сказать, что в данном случае существующая неопределенность устранена, и агент принимает решение в условиях полной информированности. В данном случае влияние внешней природы на состояние безопасности информации исключено, и оказать влияние на ее текущее состояние может только агент своим поведением.

2.4. Оценка результата

Последний блок, представленный на рис. 2, содержит модель оценки эффективности $A_{evaluation}$. Для оценки эффективности деятельности по ОБИ агентом необходимо задать набор четких качественных или количественны показателей. Данные показатели должны учитывать цели, факторы и задачи безопасности, которые ранее использовались центром на этапе формирования концепции защиты. Таким образом, возникает необходимость ввести систему показателей (метрик) безопасности $\rho\left(R_{actual}, R_{required}\right)$. Цели, факторы и задачи безопасности отображаются в систему показателей эффективности w, в которой в свою очередь вводится критерий эффективности k. Таким образом, модель оценки эффективности в общем виде представляется следующим кортежем:

$$A_{evaluation} = \left\langle \rho, R_{actual}, R_{required}, A, \Theta, W, K, W(\bullet)\right\rangle.$$

На основе полученных результатов оценки центр может вносить корректировки $\omega_M, \omega_G, \omega_F, \omega_a$ на любом из уровней данной модели управления безопасностью информации. Например, центр может внести корректировку в концепцию деятельности по обеспечению безопасности информации или, получив результаты оценки, по-новому взглянуть на состояние безопасности информации в организации, что в свою очередь может означать появление новой потребности на уровне мотивов.

3. Типы управления

Процесс формирования центром множества стратегий U можно интерпретировать как поиск альтернативных путей достижения цели и выбор из этого множества наиболее эффективного решения (рис. 3). Стратегию предлагается рассматривать как трехкомпонентную структуру, которая включает в себя: *управляющую деятельность*, *активные средства* (различного рода ресурсы, доступные центру) и *другие средства* (системы). Эффективность используемых центром стратегий также напрямую зависит от *управляемости* системы. Данное свойство характеризует способность системы переходить из одного состояния в другое за конечное (либо требуемое) время под влиянием управляющего воздействия $u(\bullet) \in U$. Иными словами, это способность оперативно реагировать на команды управления. Управляемость системы можно детализировать, оценив ее по пяти признакам: *гибкость управления, оперативность управления, точность, быстродействие и инерционность*.

Институциональное управление $u_A \in U_A$ традиционно считается наиболее жестким типом управления, поскольку его суть заключается в формировании и контроле норм и ограничений (рис. 4).

Нормы и ограничения могут быть представлены в одном из двух видов: явной форме (политика безопасности, стандарт, должностная инструкция, соглашение о конфиденциальности) и неявной (негласные правила корпоративной этики, культура информационной безопасности). Ограничения в явной форме, как правило, представлены в виде документов и носят строгий, запрещающий характер. В свою очередь, неявные формы институционального управления существуют в виде норм поведения и ценностей, принятых в организации; носят побуждающий характер.

Следует также отметить, что управление ограничениями может означать не только формирование множества допустимых действий сотрудника, но и запрет определенных действий.

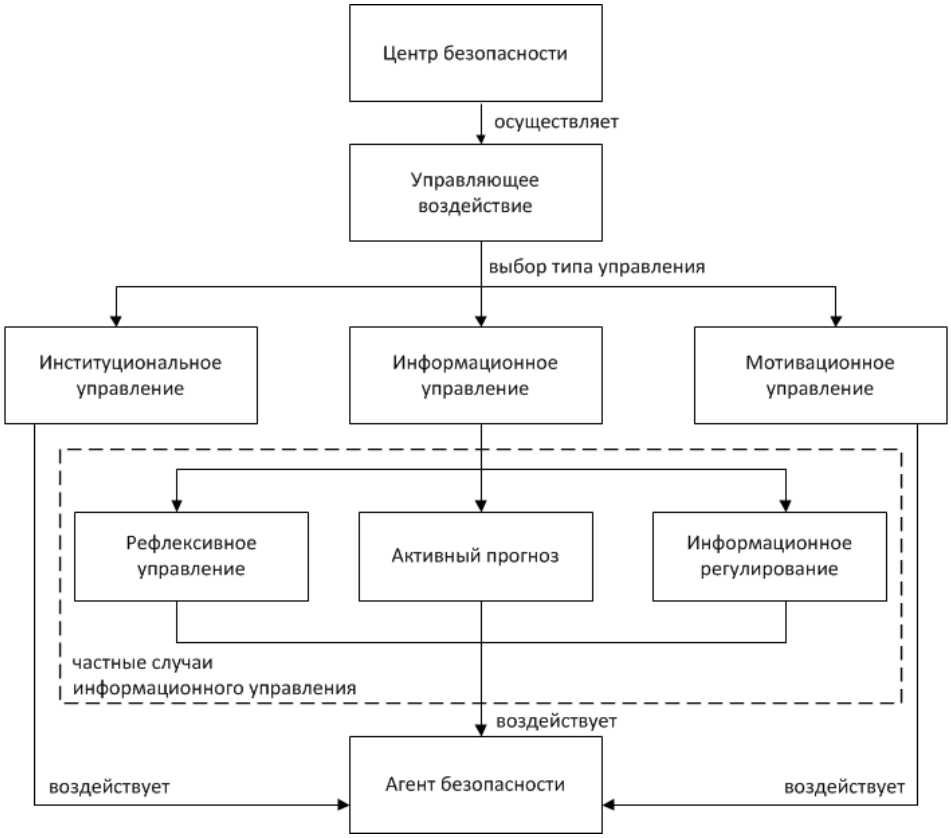

Рис. 3. Типы управления

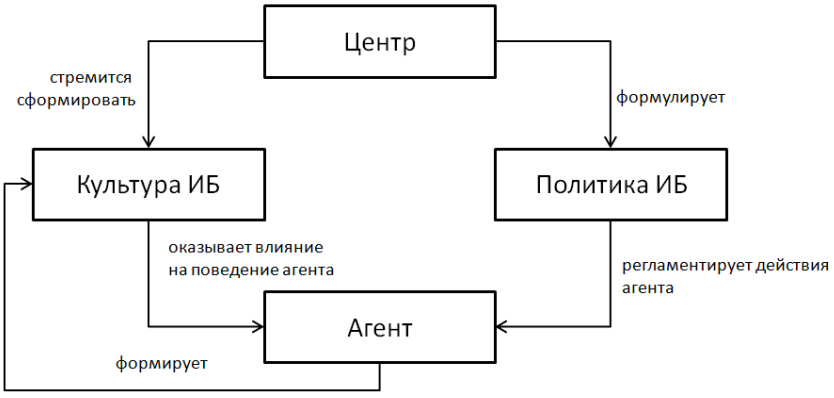

Рис. 4. Модель институционального управления в общем виде

Мотивационное управление $u_A \in U_A$, как и институциональное, заключается в целенаправленном изменении предпочтений агента на множестве возможных действий $y \in A$. Однако, в отличие от институционального, данный вид управления не ограничивает множество действий агента, а склоняет его к выбору конкретных действий, благоприятных с точки зрения центра. Такое воздействие на предпочтения агента, как правило, осуществляется через систему штрафов или поощрений за выбор необхо-

димого действия или полученный в итоге результат.

Информационное управление $u_I \in U_I$ является наименее жестким по сравнению с институциональным и мотивационным типом. При использовании данного вида управления центр сообщает агентам определенную информацию, которая влияет на их поведение и склоняет к выбору действия $y \in A$. Выделяют следующие частные случаи информационного управления:

- *Рефлексивное управление*. Центр сообщает агентам информацию о параметрах других участников организационной системы, тем самым воздействуя на представления агентов.
- *Активный прогноз*. *Центр сообщает* информацию о прогнозируемых результатах деятельности агентов.
- *Информационное регулирование*. Центр сообщает информацию о внешней обстановке, *формируя* у агента новое представление об обстановке и побуждая его к выбору благоприятного действия для центра.

Таким образом, центр играет роль управляющего органа, а агент представляет собой управляемый субъект. Рассматривая деятельность центра с позиции институционального управления, можно сформулировать задачу центра следующим образом: формирование такой политики безопасности информации (ПБ) и культуры информационной безопасности (КИБ), которые совместно будут оказывать влияние на предпочтения агента, способствуя выбору наиболее благоприятного для центра действия агента y из множества действий $y \in A$, что в свою очередь приведет к желаемому результату $r \in R_{requred}$, где результат – состояние безопасности информации в организации.

Выводы

Институциональное управление сегодня выглядит перспективным подходом к решению проблем управления нетехническими аспектами деятельности по ОБИ. Природа данного типа управления позволяет осуществлять управление как явными, так и неявными формами ограничений, накладываемых на деятельность сотрудников организации.

Предложенная модель управления учитывает следующие аспекты деятельности по ОБИ: мотивационный (потребность в защите), концептуальный (цели и задачи безопасности), функциональный (поведение агентов) и оценочный (оценивание результатов управляющих воздействий).

Активными компонентами данной модели выступают центр безопасности и агент безопасности. Деятельность агента, как было показано, оказывает значительное влияние на общее состояние безопасности информации в организации. В то же время центр, как управляющий субъект, способен формировать поведение агента при помощи необходимых управляющих воздействий. Центру доступны три основных вида управления, которые не противоречат друг другу и могут быть использованы совместно: институциональное, мотивационное и информационное.

В качестве дальнейших исследований представляется актуальным проведение более детального исследования компонент и субъектов модели институционального управления и их взаимосвязей, разработка метода оценивания неформальных компонент модели, в частности культуры информационной безопасности.

Список литературы

1. Dhillon, G. Value-focused assessment of information system security in organizations / G. Dhillon, Torkzadeh // Information Systems Journal. – 2006. –16. – P. 293-314.

2. Siponen M. A review of information security issues and respective research contributions / M. Siponen, H. Oinas-Kukkonen // SIGMIS Database. – 2007. – 38(1):– P. 60-80.

3. Vroom C. (2004). Towards information security behavioral compliance / C. Vroom, R. von Solms // Computers & Security. – 2004. – 23(3). – P. 191-198.

4. Новиков Д.А. Институциональное управление организационными системами / Д.А. Новиков. – М.: ИПУ РАН, 2004. – 68 с.

Надійшла до редколегії 20.06.2014

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МОДЕЛЬ ІНСТИТУЦІОНАЛЬНОГО УПРАВЛІННЯ ДІЯЛЬНІСТЮ ПО ЗАБЕЗПЕЧЕННЮ БЕЗПЕКИ ІНФОРМАЦІЇ

А.В. Потій, Д.Ю. Пилипенко, Д.В. Кепко

У даній статті пропонується узагальнена модель інституціонального управління інформаційною безпекою, і розглядаються її ключові компоненти: мотиваційний, концептуальний, функціональний і оціночний. Також розглянуті основні суб'єкти діяльності щодо забезпечення безпеки інформації та їх взаємозв'язок з компонентами моделі.

***Ключові слова**: інституціональне управління, центр безпеки, агент безпеки.*

THE MODEL OF INSTITUTIONAL MANAGEMENT OF ACTIVITIES FOR INFORMATION SAFETY

A.V. Potiy, D.Y. Pilipenko, D.V. Керко

In this article the generalized model of institutional management is offered by information security, and its key components are considered: motivational, conceptual, functional and estimated. The main subjects of activity on safety of information and their interrelation with model components are also considered.

***Keywords**: institutional management, safety center, agent of safety.*