УДК 378.147

УПРАВЛЕНИЕ СИНЕРГЕТИЧЕСКОЙ ОТКРЫТОСТЬЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ СОВРЕМЕННОГО ВУЗА С УЧЁТОМ ОГРАНИЧЕНИЙ НА РИСКИ

Данилов А.Н.

ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет», Пермь, Россия (614990, г. Пермь, Комсомольский проспект, 29), e-mail: dan@pstu.ru

Управление синергетической открытостью информационной системы (ИС) современного вуза с учётом ограничений на риски является существенно нелинейным процессом, характеризуемым множеством параметров в различные периоды развития вуза. При этом степень синергетической открытости выступает в качестве одного из основных параметров порядка, под которым понимается уровень доступности пользователей к заданным информационным ресурсам вуза, которую можно поставить в соответствие с определенной степенью риска, порождаемую угрозами несанкционированного (запрещенного) доступа к информации и нанесения ущерба ИС вуза. Рассматривается алгоритм управления синергетической открытостью системы при ограничениях на другие параметры порядка и скорость повышения степени открытости и приводится пример реализации предложенного алгоритма.

Ключевые слова: информационная система вуза, синергетическая открытость, степень открытости, управление синергетической открытостью, открытая и закрытая информация, время доступа, уровень информационной безопасности, риск.

MANAGEMENT OF SYNERGISTIC OPENNESS INFORMATION SYSTEM OF THE MODERN UNIVERSITY, OF UNDER RISKS LIMITATIONS

Danilov A.N.

Perm National Research Polytechnic University, Perm, Russia (614990, Perm, Komsomolsky ave., 29), e-mail: dan@pstu.ru

Management of synergistic open information system (IS) of the modern university, taking into account the limitations of the risks is essentially nonlinear process, characterized by a variety of parameters in different periods of development of the university. The degree of synergistic openness stands as one of the main parameters of the order, which refers to the level of access to users to specify the information resources of the university, which can be associated with a certain degree of risk posed by the threat of unauthorized access to information and damage IC's university. An algorithm for management of synergetic transparent systems with constraints on the other parameters of the order and the rate of openness increase are considered and an example of the implementation of the proposed algorithm is given.

Keywords: The information system of the university, synergetic openness, the degree of openness, openness synergic control, open and closed information, access time, the level of information security, risk.

Информационная система (ИС) современного вуза – это сложная организационно-техническая система, которая характеризуется большой разнородностью объектов управления и разнообразием информационных потоков между ними, а также большим числом постоянно меняющихся пользователей с различными категориями доступа к информационным ресурсам и уровнем их подготовки.

Основной задачей ИС современного вуза является информационно-аналитическое обеспечение его разноплановой деятельности, включая задачи поддержки бизнес-процессов, необходимых для функционирования структурных подразделений вуза и взаимодействия их с внешними пользователями [6].

Информационные системы вузов могут быть условно разделены на системы закрытого и открытого типа. Вуз, имеющий закрытую ИС, характеризуется чётко

выраженной внутренней структурой, слабыми контактами с внешним миром, редкой сменой персонала, отсутствием участия в обмене опытом. Как правило, подобные вузы не приемлют новых идей, концепций и методов развития, что на современном этапе не может гарантировать их конкурентоспособность на рынке образовательных услуг.

ИС вуза открытого типа динамична, открыта для совершенствования, позволяет осуществлять широкие контакты с внешним миром, увеличивает объемы доступной информации для широкого круга пользователей, а также сокращает время доступа к её информационным ресурсам. Для неё характерна высокая степень интеграции на основе информационных технологий, но в то же время она индивидуальна при реализации инновационных решений в вопросах обеспечения деятельности конкретного вуза. Подобная система постоянно взаимодействует с внешней средой, что влечёт за собой появление новых структур и новых взаимодействий между структурными элементами системы с целью компенсации этих воздействий. Как отмечается в работах [7; 8], появление новых структур и новых взаимодействий между структурными элементами системы ведёт к возникновению новых системных свойств**,** которые не могли появиться без этого объединения, поэтому при управлении открытыми системами необходимо использование синергетического подхода, позволяющего учитывать внешние воздействия на функционирование и развитие системы [4; 5; 7; 8].

Применительно к современному вузу этот подход позволяет исследовать вопросы возникновения и развития новых организационных и управленческих структур в процессе его деятельности в условиях перехода на новую парадигму образования [6], а также создания информационной системы вуза с заданными системным свойствам и характеристиками. При этом возникают вопросы - как управлять сложными открытыми образовательными системами в условиях динамических нелинейных процессов, протекающих в таких системах? Как из всего многообразия возможных состояний системы и путей её развития выбрать правильные? Как при управлении реализовывать стратегические цели развития системы, не увязнув в «мелочах» на оперативном уровне управления вузом?

Решение этой многопараметрической и многокритериальной оптимизационной задачи зависит от множества формализуемых и неформализуемых показателей и требует разработки новых подходов и методов.

В отличие от кибернетических и математических подходов, которые предполагают учёт возможно большего числа параметров и воздействий, синергетический подход, широко используемый при исследовании открытых систем, состоящих из большого количества элементов, сложным образом взаимодействующих между собой и внешней средой,

оперирует одним или несколькими так называемыми параметрами порядка системы, определяющими её поведение и развитие [6].

На наш взгляд, одним из основных параметров порядка ИС вуза является её синергетическая открытость. Известно [8], что открытость произвольной системы можно оценить с помощью некоторого параметра α, который характеризует уровень взаимодействия исследуемой системы с внешней средой и является параметром порядка при использовании синергетического подхода к управлению развитием системы в неравновесном состоянии. Данный параметр зависит от фазовых координат x элементов системы, которые описывают её состояние в данный момент времени. Поэтому в дальнейшем будем обозначать степень синергетической открытости информационной системы как $\alpha(x)$.

Отметим, что данный параметр характеризует уровень доступности пользователей к информационным ресурсам вуза, который не приводит к нарушению заданного режима функционирования ИС [1; 2].

Вследствие этого возникает проблема обеспечения информационной безопасности вуза, под которой понимается резкое увеличение рисков несанкционированного доступа к информации и нанесение невосполнимого ущерба самой ИС вуза.

Отметим, что получаемая информация существенно неоднородна по важности и величине возможного нанесенного ущерба. Каждый вид информации можно условно разбить на три группы:

1) информация открытого доступа, размещённая в общедоступных источниках информации;
2) информация ограниченного доступа, доступная в зависимости от статуса внешнего пользователя;
3) информация закрытого доступа (строго конфиденциальная).

Наличие информации ограниченного и закрытого доступа обусловливает необходимость постепенного повышения степени открытости ИС с учётом допустимых рисков её разрушения и имеющихся у вуза ресурсов, обеспечивающих устойчивость её нового состояния и конкурентноспособности на рынке образовательных услуг.

Возникает задача управления синергетической открытостью ИС вуза с учётом возможных рисков и имеющихся информационных ресурсов.

1. Оценка синергетической открытости информационной системы вуза

Процесс использования информации в вузе предусматривает периодический доступ в его ИС с целью решения задач управления различными видами деятельности [3]. При этом возникают ограничения на использование определённой части информационного ресурса,

которые будут определяться предельным временем доступа в ИС и иметь две границы: нижнюю – $T_{\max}^{\text{дост}}$ и верхнюю – $T_{\min}^{\text{защ}}$ (рис. 1).

Нижняя граница ($T_{\max}^{\text{дост}}$) является характеристикой ИС и определяет предельно допустимое время, за которое пользователь данной системы может осуществить оперативный доступ к информации и которое необходимо для решения задач управления системой или получения образовательных услуг. При этом все действия, связанные с процедурами аутентификации пользователя системой защиты, не могут превышать $T_{\max}^{\text{дост}}$, что позволяет реализовать требование к системе защиты по обеспечению предельно допустимого времени задержки пользователя на доступ к информации.

Верхняя граница ($T_{\min}^{\text{защ}}$) представляет собой предельное временное ограничение на возможность несанкционированного доступа к информационному ресурсу посредством преодоления злоумышленником механизмов защиты информации. Другими словами, система защиты информации гарантирует предельно минимальное время задержки нарушителя (злоумышленника) $T_{\min}^{\text{защ}}$.

Гарантированная защита ИС может быть обеспечена в случае выполнения следующего отношения: $T_{\max}^{\text{дост}} << T_{\min}^{\text{защ}}$. При невыполнении данного условия (либо невозможности сохранения времени доступа в ИС в заданных временных интервалах) возникают угрозы безопасности информации (конфиденциальности, целостности и доступности). Возникновение угроз безопасности информации в конечном итоге может приводить к негативным последствиям (ущербу) и оказывать влияние на показатели эффективности всей системы.

Соотношение предельных времен доступа в ИС представлено на рис. 1.

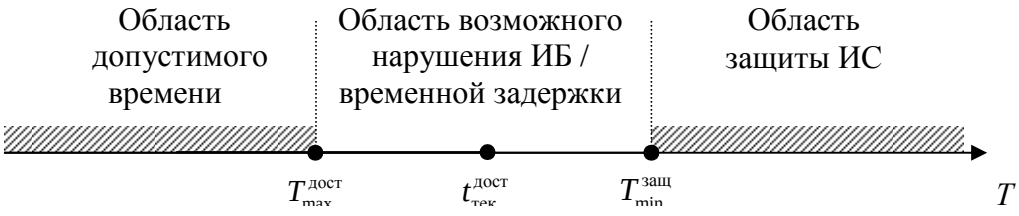

Рис. 1. Соотношение предельных времён доступа
в информационную систему.

Пусть текущее время доступа для санкционированного пользователя ИС $t_{\text{тек}}^{\text{дост}} < T_{\max}^{\text{дост}}$. Тогда степень открытости ИС определяется коэффициентом открытости α, находящимся в диапазоне $0 \le \alpha \le 1$ и определяемым соотношением

$$\alpha = 1 - t_{\text{тек}}^{\text{дост}} \Big/ \left(T_{\max}^{\text{дост}} + T_{\min}^{\text{защ}} \right). \qquad (1)$$

При $t_{\text{тек}}^{\text{дост}} \to 0$ для санкционированных пользователей ИС доступ реализуется беспрепятственно, коэффициент открытости $\alpha \to 1$.

При $t_{\text{тек}}^{\text{дост}} \to T_{\max}^{\text{дост}}$ для санкционированных пользователей ИС и при использовании информационных ресурсов ограниченного доступа последний реализуется с временной задержкой для выполнения требований безопасности информации ИС, коэффициент открытости находится в диапазоне $0 < \alpha \le 1$.

Отметим, что при функционировании ИС возникают различные риски. Под риском $R(\alpha)$ понимается степень реализации угрозы нарушения безопасности информации в ИС, вызванная нарушением порядка взаимодействия пользователя с ИС, и снижающая доступность информации при повышении степени ее конфиденциальности и целостности по причине недостаточности принимаемых мер по защите информации.

Пример взаимосвязи степени открытости α с величиной риска $R(\alpha)$ представлен на рис. 2. При необходимости увеличения степени открытости ИС с целью повышения ее доступности для отдельных категорий пользователей неизбежно возникает риск R_1, связанный с нарушением конфиденциальности и целостности информации. Это обусловлено отключением некоторых сервисов безопасности для увеличения оперативности доступа пользователей к отдельным ресурсам ИС.

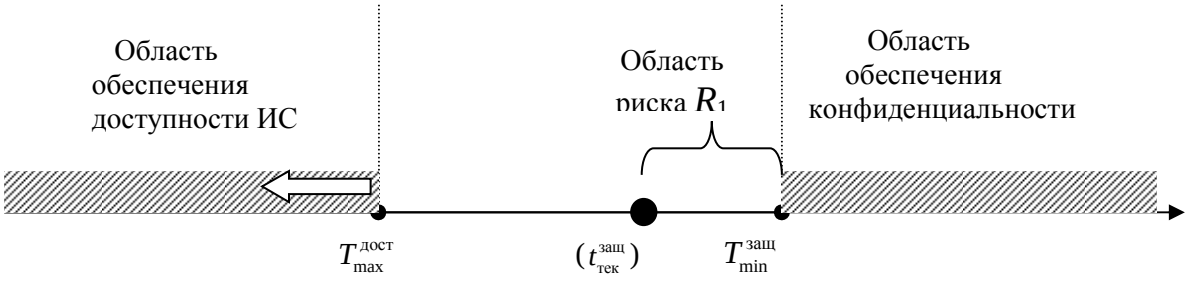

Рис. 2. Пример взаимосвязи степени открытости ИОС с риском нарушения конфиденциальности и целостности информации.

Тогда для каждого произвольного i-го взаимодействия можно определить максимально допустимую степень открытости α^*, зависящую от $T_{\max}^{\text{дост}}$ $T_{\min}^{\text{защ}}$ и ограниченную

предельной величиной риска R_i^*, т.е. $\alpha_i = f_i\left(T_{\max i}^{\text{дост}}, T_{\min i}^{\text{защ}}, R_i^*\right)$. Для решения данной проблемы необходимы постановка и решение соответствующей задачи управления.

2. Постановка задачи управления степенью открытости при ограничениях на риски

Общую постановку задачи повышения степени синергетической открытости информационной системы вуза можно сформулировать следующим образом.

Найти такие значения параметров информационной системы $x^* \in X$, которые обеспечивают максимальное значение степени её синергетической открытости:

$$\alpha(x) \to \max \tag{2}$$

при ограничениях на риски:

$$R_i(\alpha(x)) \le R_i^*, \quad i = \overline{1,m}, \tag{3}$$

где R_i^*, $i = \overline{1,m}$ – заданные значения рисков по классам информации (m – заданное количество классов).

Очевидно, что степень синергетической открытости системы определяется по её наиболее «узкому месту», т.е. по тому классу информации, риск которого максимален. Поэтому ограничения на все риски (по всем классам информации) можно заменить на ограничение по тому риску, который является максимальным, т.е. $R\ (\alpha(x)) \le R^*$, где $R^* = \max(R_i^*),\ i = \overline{1,m}$.

Однако «узкое место» в общем случае неизвестно, так как риски распределяются по классам информации, которые, кроме того, изменяются во времени. Поэтому будем считать объем общей информации равным некоторой условной единице. Тогда обозначим долю информации каждого класса в общем объеме через β_i, $i = \overline{1,m}$. Отметим, что $\beta_i \ge 0,\ \sum_{i=1}^{m} \beta_i = 1.$ Для каждого класса информации введем допустимый риск $R_i^* \in [0,1],\ i = \overline{1,m}$. При этом если $R_i^* = 0$, то для i-го класса информации риск недопустим (информация закрытого доступа) и для данного класса информации должны быть разработаны специальные средства защиты, увеличивающие общее время доступа к информации. Если $R_i^* = 1$, то в этом случае для информации открытого доступа считается, что средства защиты не нужны и время доступа к этой информации определяется только разработанными в вузе аппаратными средствами и регламентами получения электронных и бумажных документов.

Как было отмечено в разделе 1, параметр открытости ИС определяется величиной времени текущего доступа к необходимой информации и может быть записан в виде формулы (1), в которой параметры ИС представляют собой $T_{\max}^{\text{дост}}$ – максимальное (по видам информации) время доступа к информации без защиты, обусловленное существующими возможностями ИС; $T_{\min}^{\text{защ}}$ – минимальное (по видам информации и способам защиты) время защиты информации с «нулевым» риском. В дальнейшем эти параметры обозначим через x_1 и x_2.

Следует отметить, что область возможных изменений параметров x_1 и x_2 существенным образом зависит от имеющихся у вуза ресурсов, выделяемых на развитие информационной системы. Отметим, что изменение параметра x_1 требует *модернизации* всей ИС (программного обеспечения, локальных информационных сетей, организации информационных потоков и т.п.). Изменение параметра x_2 определяется существующими в вузе регламентами по защите информации, внедренными средствами защиты информации и состоянием всей ИС вуза [8].

Очевидно, что при фиксированных x_1, x_2 и $t_{\text{тек}}^{\text{дост}} \to 0$ для санкционированных пользователей ИС доступ реализуется беспрепятственно и коэффициент открытости $\alpha \to 1$.

Если $t_{\text{тек}}^{\text{дост}}$ стремится к сумме ($T_{\max}^{\text{дост}} + T_{\min}^{\text{защ}}$), система полностью закрыта и $\alpha \to 0$.

В общем случае параметр открытости находится в диапазоне $0 < \alpha < 1$.

Поэтому требуется определить такие параметры x_1 и x_2 ИС вуза, при которых выполняются все регламенты по защите информации и обеспечивается её максимальная доступность для внешних пользователей.

Остановимся подробнее на определении времени текущего доступа к необходимой информации $t_{\text{тек}}^{\text{дост}}$.

Очевидно, что для фиксированных значений x_1 и x_2 это время определяется максимально возможной степенью риска для исследуемой информационной системы $R^* = \max(R_i^*), \quad i = \overline{1,m}$ и может быть записано в виде

$$t_{\text{тек}}^{\text{дост}} = x_1 + (1 - R^*)\, x_2 . \qquad (4)$$

В случае учёта распределения информации по классам для *i*-го класса информации можно записать:

$$t_i^{\text{дост}} = x_{1i} + (1 - R_i^*)\, x_{2i}, \quad i = \overline{1,m} .$$

Следует отметить, что минимальное время, необходимое для защиты информации из *i*-й группы x_{2i}, соответствует нулевому значению риска (R_i^* = 0), а максимальное время, необходимое для доступа информации из *i*-й группы x_{1i}, соответствует максимальному риску (R_i^* =1). При этом из практики известно, что $x_{2i} >> x_{1i}$.

Теперь соотношение для степени синергетической открытости системы α, соответствующей степени риска R_i^*, примет вид

$$\alpha = (1 - \max_i(\beta_i t_i^{\text{дост}} / (x_{1i} + x_{2i})). \quad (5)$$

Рассмотрим возможные оценки α для различных ИС вуза.

1. Предположим, что вся информация в вузе находится в открытом доступе, т.е. β_1 =1, R_1^* =1 и β_i =0 $\forall i$ >1. Тогда при фиксированных значениях x_{11} и x_{21} получим оценку открытости системы в виде

$$\alpha = (1 - \beta_1 t_1^{\text{дост}} / (x_{11} + x_{21})) = (1 - x_{11} / (x_{11} + x_{21})) => 1.$$

В этом случае система является практически полностью синергетически открытой.

2. Рассмотрим противоположный случай, когда вся информация вуза находится в закрытом доступе, т.е. β_3 = 1, R_3^* = 0 и β_i = 0 $\forall i \neq 3$. Тогда получим следующую оценку открытости системы:

$$\alpha = (1 - \beta_3 t_3^{\text{дост}} / (x_{13} + x_{23})) = (1 - (x_{13} + x_{23}) / (x_{13} + x_{23})) = 0.$$

В этом случае система является синергетически закрытой.

3. Предположим, что фиксированы значения x_{1i} и x_{2i}, $\forall i$ =1,3 (*m* = 3) и требуется оценить степень открытости α.. Для определенности будем считать, что вся информация в вузе распределена по классам следующим образом: β_1 = 0,2, β_2 = 0,5, β_3 = 0,3, и заданы допустимые риски: R_1^* = 1, R_2^* = 0,2, R_3^* = 0. Кроме этого, предположим, что существующее программное обеспечение доступа информации и средства ее защиты обеспечивают соотношения $x_{2i} = 10\, x_{1i}$, $\forall i$ =1,3.

В этом случае степень открытости ИС можно оценить следующим образом:

$$\alpha = (1 - \max_i(\beta_i t_i^{\text{дост}} / (x_{1i} + x_{2i})) = 1 - \max(0,0182;\ 0,0909;\ 0,3) = 1 - 0,3 = 0,7.$$

Из приведённого примера следует, что «узким» местом открытости ИС является количество информации, отнесённой к третьему классу (закрытый доступ). Эта зависимость будет сохраняться при достаточно близком распределении информации по классам ($\beta_1 \approx \beta_2$

$\approx \beta_3$). Однако при уменьшении объема информации закрытого доступа общий уровень открытости ИС может определяться характеристиками других классов информации (в приведённой классификации частично открытой или открытой).

Например, если β_1 = 0,2, β_2 = 0,7, β_3 = 0,1, при тех же допустимых рисках получим: $\alpha = (1 - \max(0,0182;\ 0,127;\ 0,1))$ = 1 – 0,127 = 0,863, т.е. «узким» местом открытости информационной системы становится количество информации, отнесённой ко второму классу (частично открытый доступ).

Подобный результат также можно получить при увеличении риска для второго класса информации. Например, при β_1 = 0,2, β_2 = 0,6, β_3 = 0,2 и допустимом риске R_2^* = 0,4 получим:

$$\alpha = (1 - \max(0,0182;\ 0,2182;\ 0,2)) = 1 - 0,2182 = 0,7818.$$

Такой же анализ степени открытости информационной системы можно провести при различных соотношениях между x_{1i} и x_{2i}, $\forall i$ = 1, 3.

Таким образом, видно, что степень открытости ИС зависит от многих ее параметров, наиболее существенными из которых являются: распределение информации по классам (открытый доступ, частично открытый доступ, закрытый доступ), уровни допустимых рисков по этим классам информации и соотношения между временами доступа и защиты информации в каждом классе. Поэтому для каждой ИС вуза необходимо решать соответствующую оптимизационную задачу, учитывающую специфику и характеристики потоков информации, а также программно-аппаратное состояние этой ИС.

3. Демонстрационный пример решения задачи управления синергетической открытостью

Пусть задана некоторая ИС вуза, в которой вся информация разбита на три класса, характеризующиеся соответствующими параметрами: β_i, x_{1i}, x_{2i}, R_i^*, $i = \overline{1,3}$.

Введём новые переменные:

$$y_i = \beta_i (x_{1i} + (1 - R_i^*) x_{2i}) / (x_{1i} + x_{2i})), \quad i = \overline{1,3}.$$

Очевидно, что y_i характеризует открытость ИС через относительное время доступа к различной информации, распределенной на три класса.

Тогда согласно (5) синергетическую открытость ИС в некоторый момент времени *t* можно оценить следующим образом:

$$\alpha(t) = (1 - \max_i y_i(t)). \qquad (6)$$

Пусть в начальный момент времени при некотором заданном распределении β_i, x_{1i}, x_{2i}, R_i^*, $i=\overline{1,3}$ получили: $y_1(0)=0,01$, $y_2(0)=0,05$, $y_3(0)=0,7$. Тогда из (6) следует, что $\alpha(0)=1-0,7=0,3$.

Требуется найти минимальное время *T*, за которое можно повысить степень открытости данной ИС на 50%, при ограничениях на скорость изменения параметров y_i, *i* = 1, 2, 3, т.е.

$$\left|\dot{y}_i(t)\right| \le \dot{y}_{i\text{крит}},\ t\in[0,T],\ i=1,2,3. \qquad (7)$$

Эти ограничения связаны с ресурсами вуза, возможностями модернизации ИС, требованиями к защите информации и т.п.

Считаем, что заданы следующие критические скорости изменения параметров ИС вуза, при которых система не разрушается, а развивается эволюционным путём:

$$\dot{y}_{1\text{крит}}=0,02,\ \dot{y}_{2\text{крит}}=0,03,\ \dot{y}_{3\text{крит}}=0,1,$$

которые соответствуют возможностям вуза при модернизации ИС.

Исходя из соотношения (6), можно записать:

$$\dot{\alpha}(t) = -\max_i(|\dot{y}_i(t)\mid sign(\dot{y}_i(t))),\qquad t\in[0,T]. \qquad (8)$$

Предполагая монотонность по времени функций y_i, *i* = 1, 2, 3 и учитывая ограничения (7), из (8) следует, что $\dot{\alpha}(t)\le\max_i \dot{y}_{i\text{крит}}$, *i* = 1, 2, 3.

Из анализа исходных данных видно, что максимальная скорость изменения степени открытости ИС в рассматриваемом случае равна:

$$\dot{\alpha}=\dot{y}_{3\text{крит}}.$$

Подставляя исходные данные, получим значение $\dot{\alpha}$ = 0,1.

Теперь, подставляя это значение в выражение для требуемого значения параметра открытости системы в момент времени *T* ($\alpha_T=\alpha(T)$ = 0,3 · 1,5 = = 0,45) и считая справедливым предположение о линейности функции $\alpha(t)$, можно записать:

$$\alpha_T=\alpha_0+\dot{\alpha}\cdot T.$$

Тогда минимальное время *T*, за которое можно повысить степень открытости системы до требуемого значения α_T, составит:

T = (0,45 – 0,3) / 0,1 = 1,5 (года).

На рис. 3. приведено одно из возможных решений исходной задачи, соответствующее введенному предположению о линейности изменения параметров системы от времени. Очевидно, что при нелинейном характере поведения параметров ИС время модернизации системы может быть и снижено.

Следует отметить, что при найденной скорости изменения открытости системы не произойдет никаких разрушительных процессов (вследствие выполнения ограничений на ресурсы вуза).

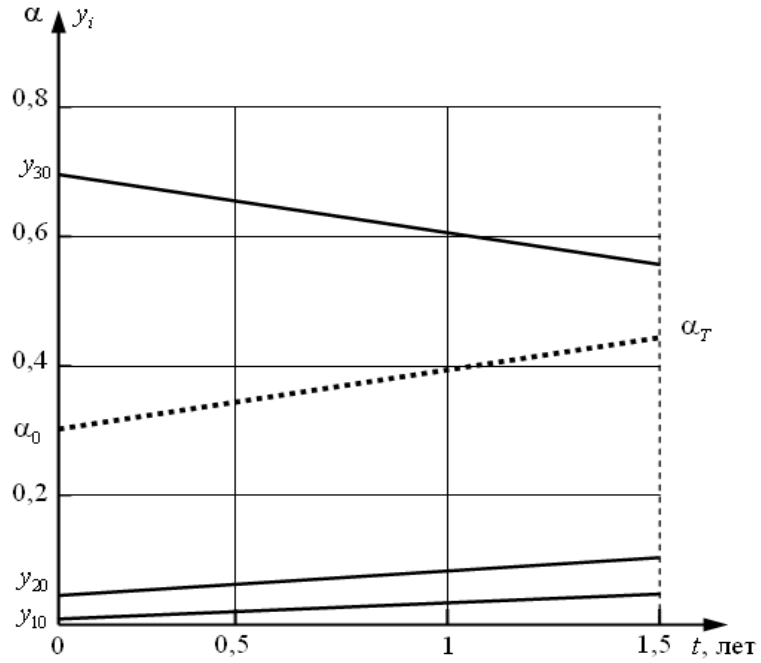

Рис. 3. Повышение степени открытости ИС вуза за счёт модернизации.

Отметим также, что в приведённом примере после модернизации ИС «узким местом» открытости доступа к информации остается третий класс, который и будет определять взаимодействие с внешними потребителями. Однако при дальнейшем снижении доли закрытой информации и модернизации ИС вуза «узкие места» могут переместиться в другие классы информации, что потребует вложения новых ресурсов вуза в повышение своей синергетической открытости.

Заключение. Показано, что процесс управления синергетической открытостью информационной системы современного вуза с учётом ограничений на риски является существенно нелинейным и требует постановки и решения многопараметрической оптимизационной задачи в различные периоды развития вуза. При этом степень открытости для заданного вида информационного ресурса можно поставить в соответствие с определенной степенью риска, порождаемую угрозами несанкционированного (запрещенного) доступа к информации и нанесения ущерба ИС вуза.

Приведённый демонстрационный пример управления показывает необходимость постепенного повышения синергетической открытости ИС вуза с учётом возможных рисков и имеющихся ресурсов вуза.

Список литературы

1. Данилов А.Н., Шабуров А.С. Концептуальный подход в решении задачи обеспечения безопасности информационно-управляющих систем // Вестник Казан. гос. техн. ун-та им. А.Н. Туполева. – 2012. – № 1 (65). – С. 113-119.
2. Данилов А.Н., Шабуров А.С. О проблеме информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – № 1. – С. 89-95.
3. Данилов А.Н., Шабуров А.С. Основные направления обеспечения информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – № 1. – С. 77-83.
4. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. - М. : Высшая школа, 1989. – 367 с.
5. Рабош В. А. Синергетический подход к проблеме устойчивого развития образования // Философия образования. – 2008. – № 2. – С. 5-12.
6. Солодова Е.А. Новые модели в системе образования: синергетический подход : уч. пособ. / предисл. Г.Г. Малинецкого. - М. : ЛИБРОКОМ, 2012. – 344 с.
7. Управление образовательной деятельностью многопрофильного технического университета на основе негэнтропийного подхода : монография / А.Н. Данилов, В.Ю. Столбов, М.Б. Гитман, В.А. Харитонов. – Пермь : Изд-во Перм. нац. исслед. политехн. ун-та, 2013. – 292 с.
8. Шаповалов В.И. Основы синергетики. Макроскопический подход. - М. : Испо-Сервис, 2000. – 312 с.

Рецензенты:

Столбов В.Ю., д.т.н., декан факультета прикладной математики и механики ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет, г. Пермь;

Гитман М.Б., д.ф.-м.н., профессор кафедры математического моделирования систем и процессов ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет, г. Пермь.