УДК 004.056

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ IT-ИНФРАСТРУКТУРОЙ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

М.В. ТУМБИНСКАЯ,
кандидат технических наук,
доцент кафедры систем
информационной безопасности
E-mail: tumbinskaya@inbox.ru
Казанский национальный исследовательский
технический университет им. А.Н. Туполева — КАИ

Вопрос управления системой защиты информации на предприятии в настоящее время чрезвычайно актуален. Это определяется и обострением проблем информационной безопасности в условиях интенсивного совершенствования технологий и инструментов защиты данных, о чем свидетельствуют рост нарушений в области защиты информации и усиление тяжести их последствий. Так, общее число нарушений в мире ежегодно увеличивается более чем на 100%, а в России число выявленных преступлений в сфере информационной безопасности возрастает ежегодно в несколько раз.

Статистика свидетельствует, что если коммерческая организация допускает утечку важной внутренней информации, то она в 60% случаев становится банкротом. Таким образом, существуют факторы и параметры, определяющие необходимость взвешенного подхода к указанной проблеме: возрастающее количество информационных угроз и рисков, недостаточный уровень обеспечения информационной безопасности существующих корпоративных информационных систем.

Необходимость обеспечения сохранности, защищенности коммерческой информации и конфиденциальных данных диктуется условиями современного рынка. Защита информационных ресурсов в деятельности современного предприятия — одно из основных направлений, которое требует проведения постоянного анализа качества применяемых средств, инструментария, методов защиты, а также их оперативного изменения и совершенствования.

В статье проанализированы проблемы целостности информации в корпоративных информационных системах, информационных ресурсов современных предприятий. Представлена формализация задачи оптимизации системы защиты информации на предприятии, определены параметры организационного управления IT-инфраструктурой в системе защиты информации на предприятии, описан контур обработки информации и принятия решений при управлении IT-инфраструктурой в системе защиты информации. Описана модель влияния «кадрового ресурса» на управление IT-инфраструктуры в системе защиты информации на предприятии. Предложены рекомендации для минимизации кадровых рисков и угроз.

Ключевые слова: *управление IT-инфраструктурой в системе защиты информации на предприятии, контур обработки информации, принятие решений, минимизация кадровых рисков и угроз*

В настоящее время получили бурное развитие информационные технологии и технические средства. Естественно, что в связи с этим системы защиты

информации (СЗИ) предприятий становятся более уязвимыми и, как следствие, предприятиям может быть нанесен значительный экономический ущерб[1]. Особое место в современной системе защиты информации предприятия имеют информационные ресурсы. Под информационными ресурсами понимаются документы и массивы документов в корпоративных информационных системах предприятия[2]. Следует отметить, что анализу защиты информации и обеспечению информационной безопасности посвятили свои исследования многие отечественные и зарубежные авторы [1, 4–9, 14, 16–21].

Расширение применения современных информационных технологий делает возможным распространение различных киберпреступлений в корпоративных информационных системах (КИС), связанных с использованием современной вычислительной техники[3]. Для активного противодействия им или хотя бы для уменьшения ущерба необходимо грамотно выбирать меры и средства обеспечения защиты информации от умышленного разрушения, кражи, порчи, несанкционированного доступа, чтения и копирования. Анализ специальной литературы [10, 11, 13] показал, что наиболее актуальными являются 3 класса проблем защиты информации в корпоративных информационных системах[4]:

1) нарушение конфиденциальности информации;

2) нарушение целостности информации;

3) нарушение работоспособности информационно-вычислительных систем (КИС).

Для решения проблем защиты целостности информационных ресурсов в корпоративных информационных системах необходимо использовать организационные меры, регламентирующие процессы функционирования КИС обработки данных, использование ее ресурсов, деятельность кадровых ресурсов, а также порядок взаимодействия пользователей в КИС. Проблема обеспечения информационной безопасности предприятия становится все более актуальной именно для российских компаний. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень[5].

Бурное развитие информационных технологий порождает новые проблемы, которые требуют незамедлительного решения. Одной из современных проблем в области защиты информации на предприятии является проблема организационного обеспечения процесса управления ИТ-инфраструктурой, которая на сегодняшний день стоит очень остро.

IT-инфраструктура предприятия — это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации. В современных условиях полнота информации, ее достоверность, скорость получения и обработки данных, эффективность информационного обмена между структурными подразделениями предприятия, оперативность принятия решений и реализации текущих задач становятся одними из наиболее значимых факторов успешности предприятия (его рентабельности, прибыльности и конкурентоспособности). Следовательно, каждое предприятие должно обеспечивать высокую степень защиты коммерческой информации, целостность своих информационных ресурсов.

Проблемы защиты информационных ресурсов возникают в связи с массовым созданием и распространением автоматизированных информационных систем. Анализ и исследования данной проблематики свидетельствуют о следующем[6]:

- наличие на предприятии утечки важной внутренней информации в объеме более 20% приводит к тому, что предприятие с вероятностью в 60% становится банкротом;
- согласно статистическим данным, 93% предприятий, лишившихся доступа к собственной информации на срок более 10 дней, прекращают заниматься экономической деятельностью.

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп.).

[2] *Хайретдинов Р.Н.* Комплексная методика оптимизации затрат на создание корпоративной системы защиты информации. М., 2011. 189 с.

[3] Техника для спецслужб. Бюро научно-технической информации. URL: http://www.bnti.ru/showart.asp?aid=288&lvl.

[4] *Казакова А.В.* Развитие системы обеспечения информационной безопасности промышленных предприятий. Самара, 2011. 181 с.; SecurityLab.Ru: информационный портал по безопасности. URL: http://securitylab.ru; Searchinform: системы защиты информации. URL: http://searchinform.ru; Компания Leta — информационная безопасность бизнеса. URL: http://leta.ru; Информационная безопасность (рынок России). URL: http://tadviser.ru.

[5] Аферы. Подделки. Криминал. URL: http://aferizm.ru/bb/it/bb_it_aktyalno_infbez.htm.

[6] Компания «Лаборатория Касперского». URL: http://kaspersky.ru; Федеральная служба по техническому и экспортному контролю (ФСТЭК России). URL: http://fstec.ru; SecurityLab.Ru: информационный портал по безопасности. URL: http://securitylab.ru; Информационная безопасность и аналитика. URL: http://ibm.com; Информационная безопасность (рынок России). URL: http://tadviser.ru.

Проведенный анализ позволяет сделать вывод о том, что, с одной стороны, существенные затраты на систему защиты информации являются необходимыми для подавляющего большинства предприятий. С другой стороны, столь же необходимым является управление IT-инфраструктурой в системе защиты информации путем оптимизации затрат на средства защиты, организации и функционирования процессов в КИС предприятия. Очевиден тот факт, что недостаточно эффективная защита или дорогостоящая защита малоценной информации является ущербом. Однако задача заключается в нахождении таких способов защиты информационных ресурсов, которые бы позволяли при заданном уровне затрат обеспечивать максимально эффективную защиту, или, наоборот, при заданном уровне защиты минимизировать затраты.

Задача оптимизации системы защиты информации предприятия становится чрезвычайно актуальной. Решение данной задачи включает следующие слагаемые:

1) определение параметров организационного управления IT-инфраструктурой в СЗИ на предприятии;

2) минимизация затрат на построение СЗИ;

3) увеличение уровня защищенности, обеспечиваемого СЗИ;

4) выбор оптимального решения по построению СЗИ на предприятии.

Условия, которые бы позволяли исключить (значительно снизить) возможность утечки информации на предприятиях, можно представить обобщенной схемой этапов работ по построению системы защиты информации (рис. 1).

Модели, методы и средства защиты информационных ресурсов, используемые на предприятиях, различны и чаще всего выбираются по правилу:

$$\langle Z \to \min, U_z \ge U_{dz} \rangle$$
$$\text{или } \langle U_z \to \max, Z \le Z_d \rangle, \quad (1)$$

где Z — затраты на разработку, реализацию, внедрение и администрирование СЗИ на предприятии;

U_z — уровень защиты, обеспечиваемый СЗИ;

U_{dz} — приемлемый уровень качества СЗИ;

Z_d — приемлемая стоимость СЗИ на предприятии.

Задачи (1) могут быть решены методами многокритериальной оптимизации, однако ограничены в практическом применении. Для решения задачи оптимизации СЗИ на предприятии предлагается использовать метод последовательных уступок[7], в котором выделяется ряд частных показателей качества защищенности, имеющих превосходство над остальными показателями, переводимыми в разряд ограничений.

Рассмотрим минимизацию затрат на построение СЗИ на предприятии. Пусть $a_{ij} = 1$, если i-е средство информационной безопасности выбрано для защиты j-го информационного ресурса предприятия, и $a_{ij} = 0$, если i-е средство информационной безопасности используется для защиты от угроз. Требуется минимизировать затраты вида:

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m} Z_{ij}a_{ij} + \sum_{i=1}^{n} Z_i k_i \to \min \quad (2)$$

при соблюдении граничных условий:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} s_j m_{ij} a_{ij} \ge U_{dz}, \ \sum_{i=1}^{n} a_{ij} = 1, \forall j \in J,$$
$$\sum_{j=1}^{m} s_{ij} = 1, a_{ij} \in \{0;1\}, \ k_{ij} \in \{0;1\}, \quad (3)$$

где Z_{ij} — затраты на защиту j-го информационного ресурса i-м средством, $i = \overline{1,n}$, $j = \overline{1,m}$; Z_i — затраты для совокупности информационных ресурсов i-м средством;

$I = \{i_1, i_2, ..., i_n\}$ – множество средств СЗИ на предприятии;

$J = \{j_1, j_2, ..., j_m\}$ – множество защищаемых информационных ресурсов;

m_{ij} — оценка качества защиты i-м средством j-го информационного ресурса;

s_j — коэффициент j-го информационного ресурса в интегрированной оценке качества СЗИ;

k_i — переменная бинарного типа, $k_i \in \{0;1\}$; $k_i = 1$, если i-е средство СЗИ может быть использовано, в противном случае $k_i = 0$.

Рассмотрим увеличение уровня защищенности, обеспечиваемого СЗИ. Требуется максимизировать уровень U_z:

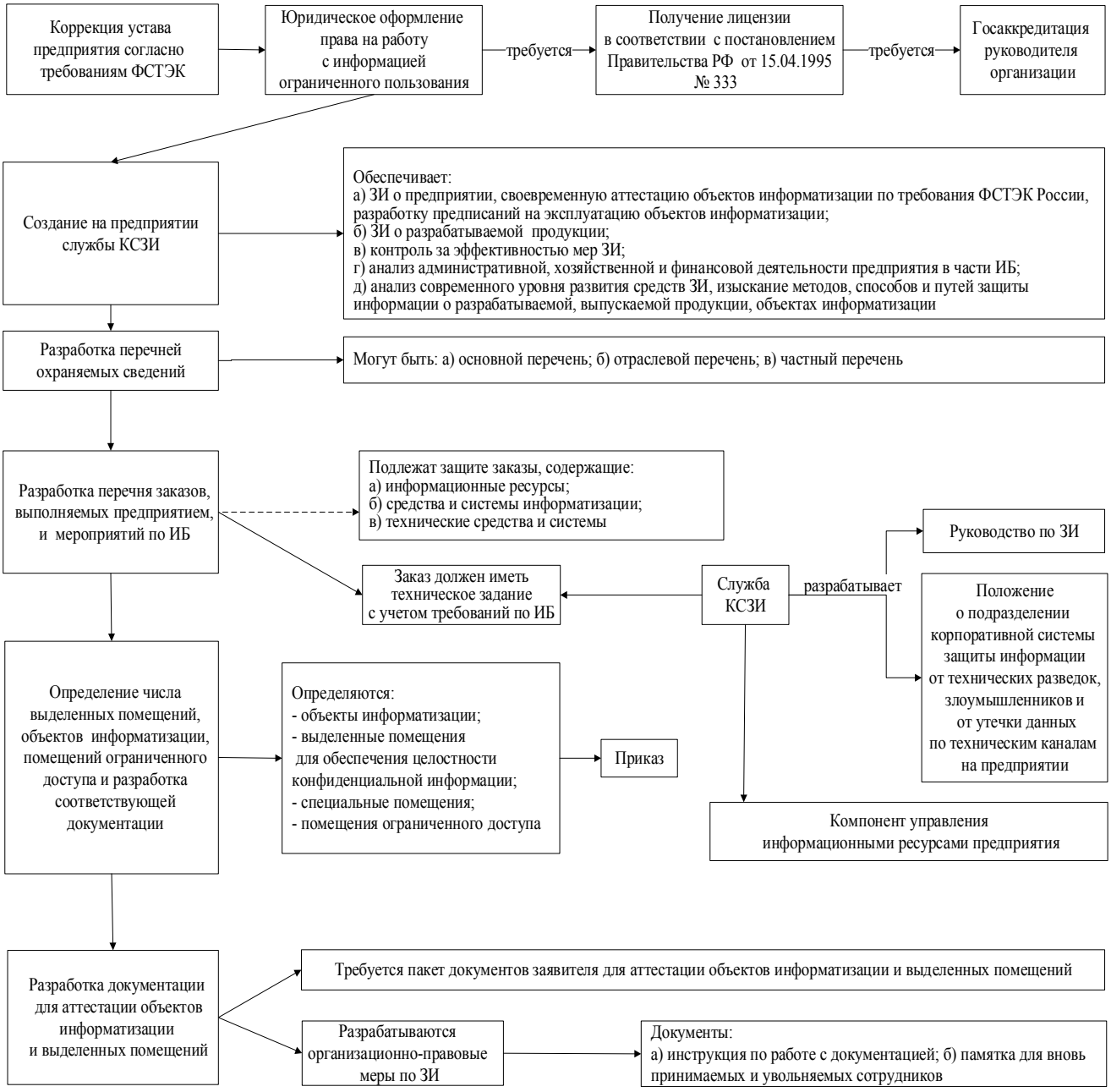
$$U_z = \sum_{i=1}^{n}\sum_{j=1}^{m} s_j m_{ij} a_{ij} \to \max \quad (4)$$

при соблюдении следующих граничных условий:

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m} Z_{ij}a_{ij} + \sum_{i=1}^{n} Z_i k_i \le Z_d, \ \sum_{i=1}^{n} a_{ij} = 1, \forall j \in J,$$
$$k_i \in \{0;1\}, a_{ij} \in \{0;1\}. \quad (5)$$

При построении интегрированной оценки уровня U_z защищенности информации, обеспечиваемого

[7] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп.).



Примечание: ФСТЭК России — Федеральная служба по техническому и экспортному контролю;
КСЗИ — корпоративная система защиты информации; ИБ — информационная безопасность; ЗИ — защита информации.

Рис. 1. Обобщенная схема этапов работ по построению СЗИ

СЗИ на предприятии, предложен следующий расчет коэффициентов защищенности отдельных бизнес-процессов $K_{b_i} = \{k_{b_1}, k_{b_2}, ..., k_{b_s}\}$ предприятия [2]:

$$K_{b_i} = 1 - \frac{\sum_{i=1}^{s} n_i \sum_{i \in P_i} \omega_{iw} y_i (1 - \Delta_w)}{\sum_{i=1}^{s} n_i \sum_{i \in P_i} \omega_{wi} y_i}, \qquad (6)$$

где P_i — количество наиболее вероятных информационных угроз для i-й бизнес-операции на предприятии;

Δ_w — коэффициент защищенности от w-й угрозы;

ω_{wi} — интенсивность потока атак w-го вида угроз на i-ю бизнес-операцию ($w \in P_i$), для $w \notin P_i$, $\omega_{wi} = 0$;

y_i — время выполнения i-й бизнес-операции;

O — количество бизнес-операций в ходе бизнес-процесса на предприятии;

n_i — вероятность выполнения бизнес-операции i в совокупности бизнес-процессов на предприятии, $O = \{o_j \mid j = \overline{1, p}\}$, $O_j \subset k_{b_i}$.

Рассмотрим выбор оптимального решения по построению СЗИ на предприятии[8]. Выбор оптимального решения по построению СЗИ на предприятии основан на анализе многопараметрического критерия, зависящего от ряда частных показателей качества работы СЗИ [12, 13]. В соответствии с формулой (1) основанием для вывода об абсолютном превосходстве одних показателей над другими служит степень различия отдельных показателей по важности, при которой сравнение оценок вариантов построения системы СЗИ осуществляется только по самому важному показателю без учета остальных, затем только по второму показателю и т.д. Таким образом, задача оптимизации сводится к задаче нахождения условного экстремума основного критерия:

$$\Omega_1 = \arg_{\gamma}\{\min_{\gamma=1,2,...,n}[c_1^{\gamma} \mid \min(c_{\phi}^{\gamma}) \le c_{\phi}^{\gamma} \le \max(c_{\phi}^{\gamma}), \phi = 1,2,...,\tau]\},$$

$$\Omega_2 = \arg_{\gamma}\{\min_{\gamma=1,2,...,n}[c_2^{\gamma} \mid \min(c_2^{\gamma}) \le c_2^{\gamma} \le \max(c_2^{\gamma}), \phi = 1,2,...,\tau]\},$$

$$\Omega_3 = \arg_{\gamma}\{\min_{\gamma=1,2,...,n}[c_3^{\gamma} \mid \min(c_3^{\gamma}) \le c_3^{\gamma} \le \max(c_3^{\gamma}), \phi = 1,2,...,\tau]\},$$

...

$$\Omega_{\tau} = \arg_{\gamma}\{\min_{\gamma=1,2,...,n}[c_{\tau}^{\gamma} \mid \min(c_{\phi}^{\gamma}) \le c_{\phi}^{\gamma} \le \max(c_{\phi}^{\gamma}), \phi = 1,2,...,\tau]\},$$

где $c_1, c_2, ..., c_{\tau}$ — частные показатели качества СЗИ;

N — общее число вариантов решений по выбору СЗИ.

С точки зрения информационной безопасности, IT-инфраструктуру целесообразно рассматривать в виде единства 3 компонентов, оказывающих взаимное влияние друг на друга:

1) информационные ресурсы;

2) технические и программные средства;

3) обслуживающий персонал и пользователи.

Согласно статистическим данным, до 80% всех возможных угроз (преднамеренных или непреднамеренных), наносимых информационным ресурсам предприятия, осуществляется пользователями КИС. Ошибочные операции или действия пользователей могут быть причиной отказа аппаратных и программных средств и системы в целом.

Для снижения информационных угроз, уязвимостей, рисков на предприятии необходим контроль и эффективное управление информационными ресурсами. Эффективное управление подразумевает принятие решений при оптимизации комплексной СЗИ на предприятии (рис. 2).

Вопросы распределения, использования и защиты информационных ресурсов предприятия возложены на службу СЗИ, которая формирует стратегию потребностей в информационных ресурсах, оценивает текущее состояние СЗИ и эффективность использования информационных ресурсов.

На предприятии защита информационных ресурсов сводится к оптимизации методов защиты информации, программных, аппаратных и технических средств.

В процессе совершенствования системы управления информационными ресурсами предприятия важную роль играет так называемый «человеческий фактор» — кадровый ресурс. Комментарии IT-компаний подтверждают информацию, что число внутренних угроз предприятия (угроз со стороны работников организации) возрастает.

Так, например, по исследованиям компании Symantec[9], основными злоумышленниками внутри предприятия являются мужчины (35–40 лет), работающие на технических должностях. Более 50% информационных ресурсов было похищено в последний месяц работы на предприятии. 75% злоумышленников похищают информацию, которая является для них открытой, т.е. они имеют к ней открытый доступ.

Опросы IT-специалистов, отвечающих за безопасность информационных ресурсов, защиту информации на предприятиях, показали, что защите данных и предотвращению утечек уделяют большое внимание 41% предприятий России. В первую тройку важных задач также вошли разработка политик восстановления IT-систем после сбоев (отметили 28% респондентов) и решение повседневных задач, связанных с обеспечением отказоустойчивости вычислительных систем (26%).

В опубликованном аналитиками отчете «Информационная безопасность бизнеса» отмечается, что наибольшее внимание организации уделяют техническим задачам, в то время как серьезные угрозы IT-безопасности в значительной мере обусловлены

[8] Федеральная служба по техническому и экспортному контролю (ФСТЭК России). URL: http://fstec.ru.

[9] Symantec: обнаружение угроз и защита информации. URL: http://symantec.com.

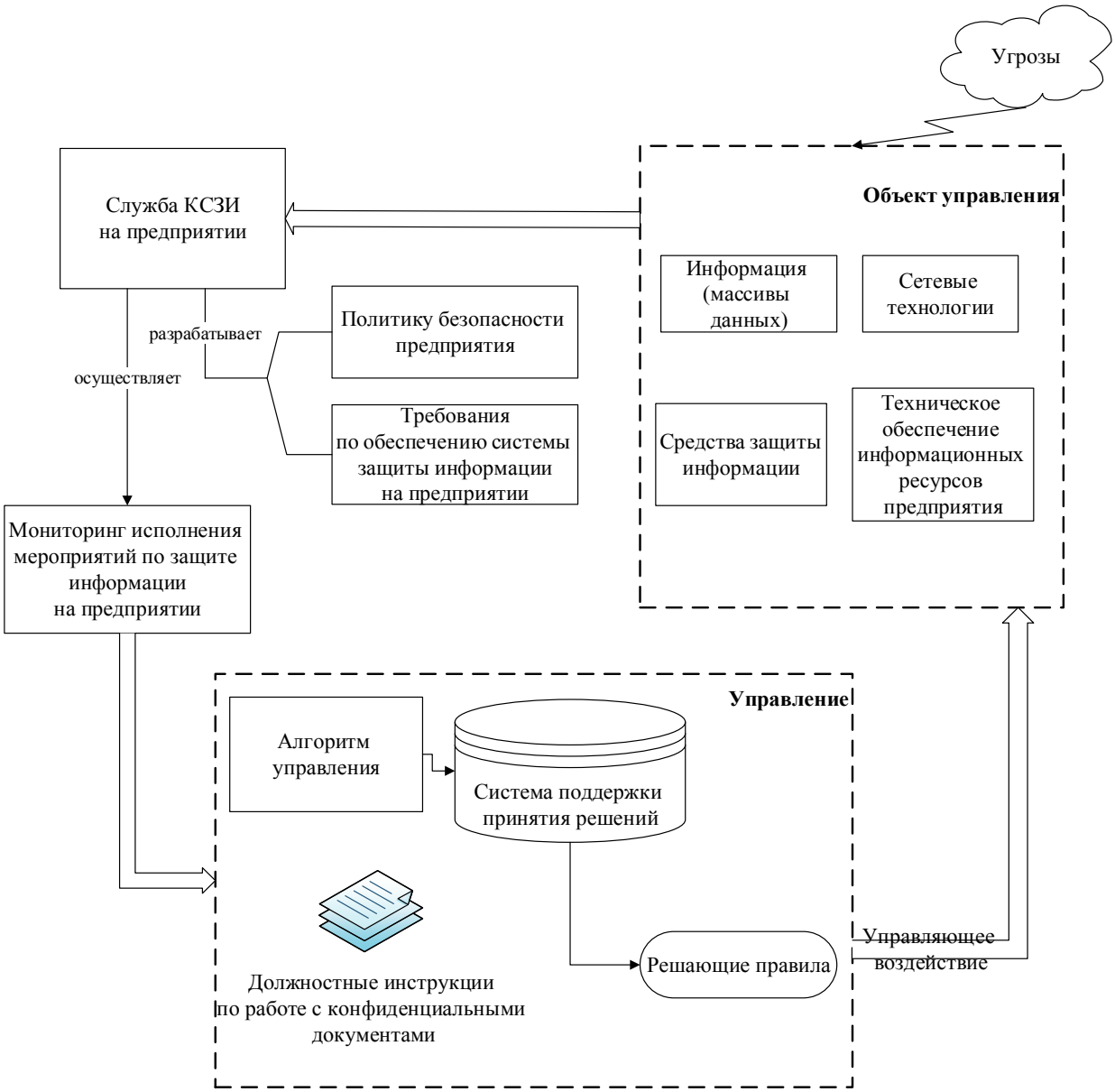


Рис. 2. Контур обработки информации и принятия решений при оптимизации СЗИ на предприятии

человеческим фактором. Так, среди 5 причин, которые приводили к утечкам данных за последний год, 3 связаны с действиями людей: 1) случайные утечки, спровоцированные сотрудниками, — 8%; 2) утечки с мобильных устройств работников — 7%; 3) корпоративный шпионаж — 7%[10]. Наиболее приоритетные задачи и проблемы, стоящие перед IT-отделами предприятий России, представлены в табл. 1.

Несмотря на постоянное совершенствование технологий защиты информационных ресурсов, человеческий фактор по-прежнему остается наиболее узким местом в системе безопасности большинства компаний. По мнению руководителя направления корпоративных продуктов в странах развивающихся рынков компании «Лаборатория Касперского» В. Удалова[11], злоумышленники умело используют пресловутый человеческий фактор.

[10] Компания «Лаборатория Касперского». URL: http://kaspersky.ru.; Информационная безопасность и аналитика. URL: http://ibm.com.; Аналитика и исследования. Информационная безопасность. Обзор рисков. Ритейл. URL: http://leta.ru.; Информационная безопасность (рынок России). URL: http://tadviser.ru.

[11] Компания «Лаборатория Касперского». URL: http://kaspersky.ru.: Информационная безопасность (рынок России). URL: http://tadviser.ru.

Таблица 1

Приоритетные задачи и проблемы, которые решали IT-отделы предприятий России в 2012 и 2013 гг., %

Задачи и проблемы	2012	2013
Защита данных, предотвращение утечек данных	40	41
Разработка политик восстановления IT-систем после сбоев	24	28
Решение повседневных задач по обеспечению отказоустойчивости IT-систем	28	26
Предотвращение инцидентов, связанных с нарушением IT-безопасности	25	25
Контроль за использованием мобильных устройств	–	22
Принятие решений о будущих инвестициях в IT-системы	29	22
Обучение пользователей работе с IT-системами	27	20
Управление изменениями в IT-системах и инфраструктуре	18	19
Понимание всего спектра новых доступных технологий и возможностей их использования	16	16
Обеспечение полного использования IT-систем для максимального возврата инвестиций (ROI)	19	16
Предотвращение ненадлежащего использования IT-систем сотрудниками	16	15
Решения для управления клиентскими системами (Client management/PC Life Cycle Management)	11	12
Управление лицензиями (на ПО, подписку, услуги)	14	11
Сложность управления продуктами различных вендоров (в том числе с несколькими консолями)	–	10
Решение вопросов, связанных с бюджетными ограничениями	13	10
Соответствие отраслевым нормативам и стандартам	11	9

Источник: по данным компании «*Лаборатория Касперского*». URL: http://www.kaspersky.ru.

Причем преступники все чаще прибегают к методам социальной инженерии, проникая в защищенные корпоративные сети через сотрудников, которые либо по незнанию, либо в силу своей беспечности, либо по злому умыслу оставляют для преступников подобные лазейки.

В общем случае модель влияния «кадрового ресурса» на управление IT-инфраструктурой в СЗИ на предприятии можно представить в следующем виде:

$K = \{I, S, P, T, D\}$, $\mu : I \times S \times P \times T \to D$,

где I — информационные ресурсы предприятия, $I = i_1, i_2, ..., i_s$;

S — множество свойств, характеризующее человеческий фактор сотрудника организации, а именно: $S = \{N, M, L, W\}$, где $N = n_1, n_2, \ldots, n_i$ — вектор, координаты которого описывают психологические свойства сотрудника; $M = \{m_j \mid j = \overline{1, p}\}$ – вектор, координаты которого описывают интеллектуальные свойства сотрудника; $L = l_1, l_2, \ldots, l_s$ — вектор, координаты которого описывают физические свойства сотрудника; $W = \{w_k \mid k = \overline{1, q}\}$ – вектор, координаты которого описывают социальные свойства сотрудника;

$P = \{0; 1\}$ — мотивация к корпоративной информационной безопасности предприятия;

T — причины, способствующие ошибочным действиям сотрудника, причем T определяется как $T = \{J, O^{\gamma}, O^{\sigma}, R, U\}$, где $J = \{0; 1\}$ — недостатки информационного обеспечения или их отсутствие (специальные обработчики таких ситуаций в программном обеспечении, наглядные материалы и инструкции). Немаловажным является параметр дефицита времени на принятие решения: $O^{\gamma} = \{o_k^{\gamma} \mid k = \overline{1, q}\}$ — ошибки, вызванные воздействием внешних факторов (отвлечение внимания от текущей задачи); $O^{\sigma} = \{o_s^{\sigma} \mid s = \overline{1, j}\}$ – ошибки, вызванные параметром S; $R = r_1, r_2, ..., r_s$ — ограниченность ресурсов поддержки и исполнения принятого решения; $U = u_1, u_2, ..., u_w$ — отсутствие учета человеческого фактора в списке возможных причин инцидента информационной безопасности;

D — уровень угрозы информационной безопасности, вызванной человеческим фактором, $D = \{d_r \mid r = \overline{1, i}\}$.

В целях совершенствования СЗИ на предприятии необходимо распределить привилегии пользователей корпоративной информационной системы. Для этого руководителю требуется провести анализ сотрудников и сформулировать рекомендации для минимизации рисков информационной безопасности и угроз, связанных с кадровым ресурсом предприятия (табл. 2).

Предложенное организационное обеспечение процесса управления IT-инфраструктурой в системе защиты информации на предприятии позволит рационально внедрить и использовать методы и средства защиты. В результате возрастет мощность информационной безопасности предприятия,

Таблица 2

Рекомендации для минимизации кадровых рисков и угроз

Рекомендации руководителю	Меры минимизации кадровых рисков и угроз
Выработать основные требования, предъявляемые к сотрудникам предприятия на предмет защиты информационных ресурсов, организовать неукоснительное выполнение требований сотрудниками	Сотрудники должны обеспечивать надлежащую защиту технических средств (персональных компьютеров), оставляемых без присмотра. Все пользователи должны знать и строго выполнять требования по безопасности информационных систем и защите технических средств, свои обязанности по обеспечению защиты информации на рабочем месте
	Сотрудникам запрещается разглашать конфиденциальную информацию при работе с информационными системами предприятия третьим лицам
	Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать к техническим средствам личные мобильные, смарт-устройства, съемные носители информации, а также записывать на них конфиденциальную информацию
	Сотрудники обязаны незамедлительно сообщать обо всех нарушениях в работе информационной системы системному администратору
	Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности информационной системы и ответственности за его нарушение
Определить качества сотрудника, которые могут способствовать утечке информации	Организация особого контроля над некоторыми категориями сотрудников: — лицами с неустойчивой психикой, низким уровнем образования, низкой мотивированностью, неудовлетворенностью материальным положением или социальным статусом; — среднего возраста (35–40 лет), не состоящими в браке; — молодого возраста (до 35 лет) с невысоким положением в коллективе предприятия и социальным статусом

увеличатся эффективность и качество принятия управленческих решений по защите информационных ресурсов.

Список литературы

1. *Власенко М.Н.* Организационные аспекты и проблемы кадрового обеспечения хозяйствующих субъектов специалистами сферы информационной безопасности в современных условиях рыночной экономики России // Национальные интересы: приоритеты и безопасность. 2011. № 24. С. 64–70.

2. *Гатчин Ю.А., Жаринов И.О., Коробейников А.Г.* Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2. С. 92–95.

3. *Горбенко И.Д., Качко Е.Г., Потий, А.В.* Решения и средства защиты информации. М.: Форум, Инфра-М, 2004. С. 528–533.

4. *Крошилин С.В.* Информационные войны на микро- и макроуровне и их влияние на экономическую безопасность // Национальные интересы: приоритеты и безопасность. 2011. № 7. С. 46–50.

5. *Карпычев В.Ю.* Экономический анализ нормативно-технического обеспечения информационной безопасности // Экономический анализ: теория и практика. 2011. № 35. С. 2–18.

6. *Коровяковский Д.Г.* Российский и зарубежный опыт в практике защиты персональных данных // Национальные интересы: приоритеты и безопасность. 2009. № 4. С. 48–54.

7. *Логинов Е.Л., Логинов А.Е.* Организационные подходы к повышению информационной безопасности систем критической инфраструктуры России // Национальные интересы: приоритеты и безопасность. 2013. № 15. С. 7–13.

8. *Логинов Е.Л., Логинов А.Е.* Проблемы повышения безопасности систем управления в ЕЭС России // Национальные интересы: приоритеты и безопасность. 2012. № 45. С. 31–37.

9. *Овсяницкая Л.Ю.* Актуальные вопросы защиты информации (на примере промышленных предприятий и учреждений здравоохранения г. Челябинска) // Национальные интересы: приоритеты и безопасность. 2013. № 21. С. 54–59.

10. *Петровский В.И., Тумбинская М.В., Петровский М.В.* Оптимизация комплексной системы защиты информации на предприятиях различных форм собственности: монография. Казань: Отечество, 2014. 636 с.

11. *Петровский В.И., Тумбинская М.В.* Принципы построения системы защиты информации на предприятиях различных форм собственности: учеб. пособие. Казань: Изд-во «Познание» Института экономики, управления и права, 2014. 469 с.

12. Помехи в технологии обеспечения информационной безопасности: монография. Казань: Изд-во КГТУ, 2004. 282 с.

13. *Петровский В.И, Петровский В.В.* Информационная безопасность и электромагнитная совместимость технических средств: монография. Казань: Изд-во КГТУ, 2005. 388с.

14. *Ревенков П.В.* Электронный банкинг: управление рисками информационной безопасности // Финансы и кредит. 2010. № 9. С. 59–63.

15. *Троников И.Б.* Методы оценки информационной безопасности предприятия на основе процессного подхода. СПб: СПбГУ ИТМО, 2010. 134 с.

16. *Терентьев А.М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. № 33. С. 37–42.

17. *Устинович Е.С., Барбашин Е.А.* Правовые гарантии обеспечения информационной безопасности при осуществлении информационной деятельности органами публичной власти в России // Национальные интересы: приоритеты и безопасность. 2008. № 3. С. 84–88.

18. *Царегородцев А.В.* Анализ рисков безопасности данных в корпоративных сетях кредитно-финансовых организаций на основе облачных вычислений // Национальные интересы: приоритеты и безопасность. 2013. № 39. С. 35–43.

19. *Чумичкин А.А.* Современные вызовы развитию информационных технологий в условиях использования сетевых сообществ в реализации стратегий информационных войн // Национальные интересы: приоритеты и безопасность. 2012. № 9. С. 33–41.

20. *Шиндин А.И.* Информационноя безопасность как решающий фактор для достижения бизнес-целей // Национальные интересы: приоритеты и безопасность. 2008. № 5. С. 70–72.

21. *Юрьева Л.В.* Особенности и проблемы системы информационной безопасности в металлургических холдингах // Национальные интересы: приоритеты и безопасность. 2008. № 10. С. 74–80.

National interests: priorities and security ***Threats and security***
ISSN 2311-875X (Online)
ISSN 2073-2872 (Print)

ORGANIZATIONAL SUPPORT TO IT INFRASTRUCTURE MANAGEMENT IN THE INFORMATION SECURITY SYSTEM OF AN ENTERPRISE

Marina V. TUMBINSKAYA

Abstract

At present, the issue of information security management of an enterprise is extremely relevant. Its relevance is determined by aggravating problems of information security in the conditions of intensive improvement of data protection technologies and tools. It is proved by increased number of violations in the field of information protection and growing seriousness of their consequences. Globally, the total annual number of violations increases by more than 100%. In Russia, the number of reported crimes in the sphere of information security increases several times every year. The statistics shows that if a commercial organization leaks important internal information, it becomes a bankrupt in 60% of cases. Thus, there are factors and parameters that determine the need for a balanced approach to the indicated problem: the growing number of data-related threats and risks, inadequate information security of existing corporate information systems. The modern market dictates the need to ensure security and protection of commercial information and sensitive data. Protection of information resources at modern enterprises is one of the main areas, which requires a continuous analysis of the quality of resources, tools, security methods, as well as their prompt update and improvement. The article analyses the challenges to information integrity in corporate information systems, and information resources of modern enterprises. The author offers formalization of information security system optimization of an enterprise. The paper defines organizational management parameters of the IT infrastructure in the data security system of an enterprise, describes the information-processing procedure and decision-making while managing IT infrastructure within the information security system. The author describes a model of "personnel resource" influence on IT infrastructure management in the system of data protection of an enterprise and offers recommendations to minimize human resource risks and threats.

Keywords: IT infrastructure management, enterprise information security, contour information processing, decision making, minimizing personnel risks, threats

References

1. Vlasenko M.N. Organizatsionnye aspekty i problemy kadrovogo obespecheniya khozyaistvuyushchikh sub"ektov spetsialistami sfery informatsionnoi bezopasnosti v sovremennykh usloviyakh rynochnoi ekonomiki Rossii [Organizational aspects and problems of staffing economic agents with specialists in the field of information security under Russian current economic environment]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2011, no. 24, pp. 64–70.

2. Gatchin Yu.A., Zharinov I.O., Korobeinikov A.G. Matematicheskie modeli otsenki infrastruktury sistemy zashchity informatsii na predpriyatii [Mathematical models of assessing the infrastructure of information security systems of an enterprise]. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki = Scientific and Technical Journal of Information Technologies, Mechanics and Optics,* 2012, no. 2, pp. 92–95.

3. Gorbenko I.D., Kachko E.G., Potii A.V. *Resheniya i sredstva zashchity informatsii* [Information security solutions and tools]. Moscow, Forum, INFRA-M Publ., 2004, pp. 528–533.

4. Kroshilin S.V. Informatsionnye voiny na mikro- i makrourovne i ikh vliyanie na ekonomicheskuyu bezopasnost' [Information warfare at micro- and macrolevels and their impact on economic security]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2011, no. 7, pp. 46–50.

5. Karpychev V.Yu. Ekonomicheskii analiz normativno-tekhnicheskogo obespecheniya informatsionnoi bezopasnosti [Economic analysis of normative-technical support for information security]. *Ekonomicheskii analiz: teoriya i praktika = Economic analysis: theory and practice,* 2011, no. 35, pp. 2–18.

6. Korovyakovskii D.G. Rossiiskii i zarubezhnyi opyt v praktike zashchity personal'nykh dannykh [The Russian and foreign experience in the practice of personal data protection]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2009, no. 4, pp. 48–54.

7. Loginov E.L., Loginov A.E. Organizatsionnye podkhody k povysheniyu informatsionnoi bezopasnosti sistem kriticheskoi infrastruktury Rossii [Organizational approaches to enhancing information security systems of the Russian critical infrastructure]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2013, no. 15, pp. 7–13.

8. Loginov E.L., Loginov A.E. Problemy povysheniya bezopasnosti sistem upravleniya v EES Rossii [Problems of enhancing management system safety in the UES of Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2012, no. 45, pp. 31–37.

9. Ovsyanitskaya L.Yu. Aktual'nye voprosy zashchity informatsii (na primere promyshlennykh predpriyatii i uchrezhdenii zdravookhraneniya g. Chelyabinska) [Topical issues of information security (the case of Chelyabinsk industrial enterprises and health care institutions)]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2013, no. 21, pp. 54–59.

10. Petrovskii V.I., Tumbinskaya M.V., Petrovskii M.V. *Optimizatsiya kompleksnoi sistemy zashchity informatsii na predpriyatiyakh razlichnykh form sobstvennosti: monografiya* [Optimization of comprehensive system of information security at enterprises with various forms of ownership: a monograph]. Kazan, Otechestvo Publ., 2014, 636 p.

11. Petrovskii V.I., Tumbinskaya M.V. *Printsipy postroeniya sistemy zashchity informatsii na predpriyatiyakh razlichnykh form sobstvennosti: uchebnoe posobie* [Principles of building information security system at enterprises with various forms of ownership: a textbook]. Kazan, Poznanie Publ., 2014, 469 p.

12. *Pomekhi v tekhnologii obespecheniya informatsionnoi bezopasnosti: monografiya* [Hazards in the technology of information security support: a monograph]. Kazan, Kazan State Technical University Publ., 2004, 282 p.

13. Petrovskii V.I, Petrovskii V.V. *Informatsionnaya bezopasnost' i elektromagnitnaya sovmestimost' tekhnicheskikh sredstv: monografiya* [Information security and electromagnetic compatibility of technical equipment: a monograph]. Kazan, Kazan State Technical University Publ., 2005, 388 p.

14. Revenkov P.V. Elektronnyi banking: upravlenie riskami informatsionnoi bezopasnosti [Electronic banking: information security risk management]. *Finansy i kredit = Finance and credit,* 2010, no. 9, pp. 59–63.

15. Tronikov I.B. *Metody otsenki informatsionnoi bezopasnosti predpriyatiya na osnove protsessnogo podkhoda* [Methods of assessing information security of an enterprise based on the process approach]. St. Petersburg, Saint Petersburg State University of Information Technologies Publ., 2010, 134 p.

16. Terent'ev A.M. Vybor adekvatnykh sredstv informatsionnoi zashchity personal'nogo komp'yutera v Rossii [Choosing appropriate information security tools for personal computers in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2012, no. 33, pp. 37–42.

17. Ustinovich E.S., Barbashin E.A. Pravovye garantii obespecheniya informatsionnoi bezopasnosti pri osushchestvlenii informatsionnoi deyatel'nosti organami publichnoi vlasti v Rossii [Legal guarantees to ensure information security when implementing information activities by public authorities in Russia]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2008, no. 3, pp. 84–88.

18. Tsaregorodtsev A.V. Analiz riskov bezopasnosti dannykh v korporativnykh setyakh kreditno-finansovykh organizatsii na osnove oblachnykh vychislenii [Analyzing data security risks in corporate networks of credit and financial institutions on the basis of cloud computing]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2013, no. 39, pp. 35–43.

19. Chumichkin A.A. Sovremennye vyzovy razvitiyu informatsionnykh tekhnologii v usloviyakh ispol'zovaniya setevykh soobshchestv v realizatsii strategii informatsionnykh voin [Today's challenges faced by IT development under conditions of using online communities in information warfare strategy implementation]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2012, no. 9, pp. 33–41.

20. Shindin A.I. Informatsionnoya bezopasnost' kak reshayushchii faktor dlya dostizheniya biznes-tselei [Information security as a crucial factor to achieve business goals]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2008, no. 5, pp. 70–72.

21. Yur'eva L.V. Osobennosti i problemy sistemy informatsionnoi bezopasnosti v metallurgicheskikh kholdingakh [Features and problems of information security system in metallurgical holdings]. *Natsional'nye interesy: prioritety i bezopasnost' = National interests: priorities and security,* 2008, no. 10, pp. 74–80.

Marina V. TUMBINSKAYA
Kazan National Research Technical University
named after A.N. Tupolev —
Kazan Aviation Institute,
Kazan, Russian Federation
tumbinskaya@inbox.ru