

КАЧЕСТВО ИННОВАЦИИ ОБРАЗОВАНИЕ

№6
2011



журнал в журнале

КАЧЕСТВО и ИПИ (CAL S)-технологии

www.quality-journal.ru

ГЛАВНЫЙ РЕДАКТОР
ОБЪЕДИНЕННОЙ РЕДАКЦИИ
Азаров В.Н.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Алешин Н.П., Бойцов Б.В., Бородулин И.Н.,
Быков Д.В., Васильев В.А., Васильев В.Н.,
Викторов А.Д., Домрачев В.Г., Жичкин
А.М., Журавский В.Г., Карабасов Ю.С.,
Карцев Е.А., Киринок А.А., Кондрашов
П.Е., Кортов С.В., Кофанов Ю.Н., Кеменов
В.Н., Лопота В.А., Леохин Ю.Л., Львов Б.Г.,
Малышев Н.Г., Марин В.П., Митрофанов
С.А., Мищенко С.В., Неволин В.Н., Олей-
ник А.В. (зам. главного редактора), Патраков
Н.Н., Петров А.П., Рапопорт Б.М., Сергеев
А.Г., Скуратов А.К., Смакотина Н.Л.,
Старых В.А., Степанов С.А., Стриханов М.Н.,
Строитель В.Н., Суворин А.В. (шеф-
редактор «Качество и ИПИ (CALS)-техноло-
гии»), Судов Е.В., Тихонов А.Н., Фирстов
В.Г., Харин А.А., Харламов Г.А., Храменков
В.Н., Червяков Л.М., Шленов Ю.В.

ЗАРУБЕЖНЫЕ ЧЛЕНЫ РЕДКОЛЛЕГИИ
Диккенсон П., Зайчек В., Иняц Н.,
Кэмпбелл Д., Лемайр П., Одфилд Э.,
Пулиус М., Роджерсон Д., Фарделф Д.

АДРЕС РЕДАКЦИИ И ИЗДАТЕЛЯ
109028, Москва, Большой Трехсвятительский
пер., д. 3/12
Тел.: +7 (495) 916-28-07, +7 (495) 916-8929,
факс: +7 (495) 916-8865
E-mail: quality@miem.edu.ru (для статей),
pii@miem.edu.ru (по общим вопросам)
www.quality-journal.ru; www.quality21.ru

УЧРЕДИТЕЛИ
Российский государственный
университет инновационных технологий
и предпринимательства (РГУИТП)
Московский государственный институт
электроники и математики (МИЭМ)
МАТИ – «Российский государственный
технологический университет
им. К.Э. Циолковского»
«Европейский центр по качеству»

ПРЕДСЕДАТЕЛЬ СОВЕТА УЧРЕДИТЕЛЕЙ
Быков Д.В.

ИЗДАТЕЛЬ
Европейский центр по качеству

НАУЧНЫЙ РЕДАКТОР
Леохин Ю.Л.

АВТОР ДИЗАЙН-ПРОЕКТА
Логинов К.В.

ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ
Савин Е.С.

ЖУРНАЛ ЗАРЕГИСТРИРОВАН
в Министерстве РФ по делам печати,
телерадиовещания и средств массовых
коммуникаций. Свидетельство о регистрации
ПИ № 77-9092.

ПОДПИСНОЙ ИНДЕКС
в каталоге агентства «Роспечать» 80620, 80621;
в каталоге «Пресса России» 14490.

ОТПЕЧАТАНО
«Полиграфическая компания «Принтико»», Москва,
ул. Краснобогатерская, д. 6, www.sts-print.ru

© «Европейский центр по качеству», 2011

Журнал входит в перечень ВАК РФ

Статьи рецензируются

Журнал выходит при содействии
Министерства образования и науки РФ
Журнал осуществляет информационную
поддержку научно-технических программ
и научно-технических мероприятий
Министерства образования и науки РФ

СОДЕРЖАНИЕ

ОБЩИЕ ПРОБЛЕМЫ ОБРАЗОВАНИЯ

А.Г. СЕРГЕЕВ, Ю.И. ЗАХАРОВ
О методиках государственной оценки деятельности
образовательного учреждения и общественно-профессиональной аккредитации
образовательных программ 2

Г.А. ФИРСОВ, М.Г. СЕРГЕЕВА
Формирование навыков самостоятельной работы по правовому курсу
у обучающихся как инновационный подход в профессиональном образовании 4

Ю.В. ГРИГОРЬЕВ, К.В. ПРОХОРЕНКО
Выявление и индивидуальное обучение молодежи со склонностью к техническому
творчеству 8

МЕНЕДЖМЕНТ КАЧЕСТВА И ИННОВАЦИОННЫЙ МЕНЕДЖМЕНТ

В.В. МАРТЫНОВ, И.Э. ВЕДЕНЯПИН, З.А. ДАВЛЕТОВА
Оценка качества в рамках типового ЛПУ как элемент информационной системы
менеджмента качества 13

А.М. ПОГОСЯН
Гармонизация процессов создания наукоемких объектов машиностроения
на принципах менеджмента качества 18

КАЧЕСТВО И ИПИ (CALS)-ТЕХНОЛОГИИ

КАЧЕСТВО: РУКОВОДСТВО, УПРАВЛЕНИЕ, ОБЕСПЕЧЕНИЕ

Б.Е. НЕДБАЙЛЮК
Семь необходимых действий для организации внутренних аудитов качества 23

ПРИБОРЫ, МЕТОДЫ И ТЕХНОЛОГИИ

А.В. МАСЛОБОЕВ
Метод комплексной оценки эффективности слабо формализованных этапов
жизненного цикла инноваций на основе теории нечетких множеств 28

В.К. ФЕДОРОВ, К.С. ГУЖЕВКИН
Статистический метод прогнозирования показателей качества приборных корпусов
радиоэлектронных средств 36

А.В. ИВАНОВ, В.В. ЖАБИНСКИЙ
Реализация симметричных алгоритмов шифрования ГОСТ 28147-89 и ZDES
в одном устройстве 40

Н.А. МЕШКОВ
Методика качественного анализа инновационных процессов, происходящих
в информационно-коммуникационном медико-производственном пространстве 44

Ш.А. ДЖАБРАИЛОВ
Модель сложного опциона на базе диффузионно-скачкового процесса Пуассона
для целей оценки стоимости НИОКР в фармацевтическом секторе 48

КАЧЕСТВО ОКРУЖАЮЩЕЙ СРЕДЫ

А.В. ГОРДИЕНКО
Чем привлекателен Киотский протокол для российского бизнеса? 52

ВНЕДРЕНИЕ ИПИ (CALS)-ТЕХНОЛОГИЙ

Н.К. ТРУБОЧКИНА
Разработка и моделирование качественно новой 3D наноструктуры КМОП инвертора
с проектной нормой 20 нм – основы новой элементной базы энергосберегающих СБИС 58

ТЕХНОЛОГИИ УПРАВЛЕНИЯ ДАННЫМИ

С.С. ВЕЛИГОДСКИЙ, В.А. ФИЛИППОВ
Система информационной безопасности корпоративных порталов:
критерий эффективности и ограничения 64

А.Д. КАЛУЖСКИЙ
Каталогизация изделий: вопросы сопоставительного анализа 67

ЭКОНОМИКА И УПРАВЛЕНИЕ

Ю.А. АРУТЮНОВ
Контроллинг в системе повышения качества управления организацией 75

С.С. Велигодский, В.А. Филиппов

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ПОРТАЛОВ: КРИТЕРИЙ ЭФФЕКТИВНОСТИ И ОГРАНИЧЕНИЯ

Рассмотрены проблемы обеспечения информационной безопасности корпоративных порталов. Определена актуальность задачи обеспечения информационной безопасности корпоративных порталов. Описано взаимодействие двух противодействующих систем - нарушителя и системы защиты. Сформулированы основные подходы к выбору критерия эффективности, количества и состава оцениваемых параметров, а также аналитические соотношения, описывающие модель взаимодействия, генеральную целевую функцию для оценки эффективности и ресурсные ограничения.

Ключевые слова: информационная безопасность, корпоративные порталы, уязвимость

Постоянно растущая информатизация общества и повышение ценности информации приводят к необходимости совершенствования методов и средств защиты информации и противодействия угрозам нарушения информационной безопасности (ИБ). В рамках информатизации всех сфер деятельности общества и государства осуществляется активное применение информационных ресурсов (ИР), обеспечивающих внутренние бизнес-процессы функционирования организаций и представляющих собой территориально распределенную неоднородную информационную среду (интранет), построенную на базе современных веб-технологий и клиент-серверных архитектур. Задачи управления, поддержки и доступа к ИР интранета решаются путем создания корпоративного портала (КП) — единого интерфейса доступа к различным сервисам и приложениям Интранет-среды. Эффективность КП для решения данных задач обусловлена широким применением современных Интернет-технологий (SOA-архитектура, веб-сервисы, HTTP-протоколы доступа, динамический контент и пр.). Опыт промышленных предприятий всего мира свидетельствует, что предприятия, применяющие ИТ-инфраструктуру в виде интранета, имеют безусловные конкурентные преимущества благодаря существенному снижению операционных затрат, сокращению времени на обработку заказов, усилению по-

зиций при ведении переговоров с поставщиками и потребителями.

Вместе с тем КП существенно увеличивает угрозы нарушения ИБ ИР интранета. Это обусловлено тем, что ранее доступ к корпоративным приложениям контролировался на сетевом и прикладном уровнях. При внедрении КП информационное взаимодействие осуществляется через единственный общедоступный порталный интерфейс, контролируемый на прикладном уровне. При этом КП предоставляет интерфейсы для взаимодействия как сотрудников (внутренних пользователей КП), так и внешних пользователей (посетителей, клиентов, партнеров и пр.) через публичные сети (Интернет и пр.), среди которых могут находиться потенциальные злоумышленники. Унификация технологий организации доступа к ИР и использование для этого «слабых», с точки зрения ИБ, веб-технологий упрощает для потенциальных злоумышленников возможности реализации угроз нарушения ИБ.

Следовательно, с точки зрения ИБ, КП является центральным компонентом Интранет-среды, поражение которого приведет к потерям (материальным или нематериальным) для его владельцев и пользователей. Массовый доступ пользователей к ресурсам КП, уязвимости в системном и прикладном программном обеспечении (СПО и ППО), некорректный выбор архитектуры порталного решения, неправиль-

S.S. Veligodsky, V.A. Filippov

INFORMATION SECURITY SYSTEM: AN EFFICIENTLY CRITERIA AND RESTRICTIONS

The problems of information security of enterprise portals are considered. Relevance of task of enterprise portals information security provision is defined. The process of interaction of two counteracting systems (the intruder and the security system) is described. The general mathematical expressions, describing model of interaction and resource restrictions, are formulated.

Keywords: information security, enterprise portals, security threats, interaction model, vulnerability

ная конфигурация используемых систем и сервисов – все это существенно увеличивает угрозы нарушения ИБ КП. В связи с этим построение портального решения должно быть тесно связано с комплексом мероприятий по его ИБ. Причем стало очевидным, что использование системами обеспечения информационной безопасности (СИБ) жестких, наперед заданных алгоритмов функционирования бесперспективно. Более эффективен алгоритм поведения СИБ, основанный на адаптивном управлении. Данная стратегия защиты позволяет своевременно обнаруживать события, потенциально влияющие на ИБ, и реагировать на них в режиме реального времени (или близком к нему), используя правильно спроектированные, эффективно управляемые процессы и средства его ИБ. Такой подход основан на принципе рационального поведения. Его отличительной особенностью является поиск рациональных алгоритмов поведения систем, предполагающих активные упреждающие действия и гибкое реагирование, основанное на учете особенностей ситуации и поступающей информации об угрозах нарушения ИБ.

Очевидно, что в процессе противодействия угрозам нарушения ИБ КП во взаимодействии находятся две системы: система S_1 – атакующая система со средствами нарушения ИБ КП, обеспеченная необходимыми техническими средствами для реализации угроз нарушения ИБ КП (система нарушения ИБ – СНИБ); система S_2 – объект нападения – КП с соответствующими средствами его ИБ (система обеспечения ИБ – СИБ).

Каждая из взаимодействующих систем в момент времени t_k характеризуется множеством параметров в пространстве фазовых состояний систем:

- система S_1 – множеством параметров: $Z_k^1 = [Z_{1k}^1, Z_{2k}^1, \dots, Z_{ik}^1, \dots, Z_{jk}^1] = \{Z_{ik}^1\}, i = 1(1)I$, определяющих количество возможных угроз нарушения ИБ КП;
- система S_2 – множеством параметров: $Z_k^2 = [Z_{1k}^2, Z_{2k}^2, \dots, Z_{jk}^2, \dots, Z_{jk}^2] = \{Z_{jk}^2\}, j = 1(1)J$, определяющих наличие и состояние средств защиты в СОИБ КП.

Конфликтное взаимодействие систем опишем как процесс их взаимного воздействия с помощью системы многошаговых уравнений:

$$\begin{cases} Z_{k+1}^1 = \varphi_1(Z_k^1, u_k^1, v_k^1, \Lambda) \\ Z_{k+1}^2 = \varphi_2(Z_k^2, u_k^2, v_k^2, \Lambda) \\ Z_0^1 = Z_{исх}^1 \\ Z_0^2 = Z_{исх}^2 \\ k = 0(1)K - 1, \end{cases} \quad (1)$$

где Z_k^1 – траектория процесса смены состояний S_1 до момента $t_{k,n}$, $Z_k^1 = \{z_0, z_1, \dots, z_k\}$; Z_k^2 – траектория процесса смены состояний S_2 до момента $t_{k,n}$, $Z_k^2 = \{z_0, z_1, \dots, z_k\}$; u^k, v^k – совокупность управляющих воздействий систем S_1 и S_2 соответственно до момента $t_{k,n}$, $u^k = \{u_0, u_1, \dots, u_k\}, u^k \in U$, $v^k = \{v_0, v_1, \dots, v_k\}, v^k \in V$, U, V – множества возможных взаимных воздействий систем S_1 и S_2 соответственно; $Z_{исх}^1, Z_{исх}^2$ – исходные состояния систем, k – количество шагов взаимодействия систем; Λ – возмущающие воздействия внешней среды.

Управляющие воздействия v^k, u^k являются, соответственно, внутренними и внешними для системы S_2 . При этом u^k представляет собой фактор "поведенческой" неопределенности. Фактически U определяется средствами, используемыми злоумышленником для реализации атаки на КП, V – механизмами защиты. Например, при рассмотрении атаки на КП с использованием специализированного сканера уязвимостей (XSpider, Nikto, Nessus и пр.) и обеспечения ИБ КП штатными средствами U определяется функциональными возможностями самого сканера, его БД уязвимостей, наличием дополнительных средств использования уязвимостей, а V – средствами ИБ КП: идентификацией, аутентификацией, авторизацией, мониторингом и аудитом.

Каждая из систем в ходе конфликта способна реализовать некоторую последовательность воздействий:

$$\begin{aligned} u &= \{u^0, u^1, \dots, u^k\}, \\ v &= \{v^0, v^1, \dots, v^k\}. \end{aligned}$$

Для этих воздействий можно говорить об эффективности (успешности) воздействия, под которой понимается соответствие реального результата воздействия требуемому, с точки зрения воздействующей системы (S_1 или S_2).

С точки зрения оценки эффективности функционирования систем (в рамках рассматриваемого конфликтного взаимодействия – эффективности управляющих воздействий) имеются текущие и интегральные показатели, определяемые как среднее значение функции соответствия f^{i2} реального результата, достигнутого системой к оцениваемому моменту времени:

$$\begin{aligned} W_{k+1}^1 &= M[f_{k+1}^1(Y_{k+1}^1, Y_{mp}^1)] \\ W_{k+1}^2 &= M[f_{k+1}^2(Y_{k+1}^2, Y_{mp}^2)] \\ W^1 &= M[f^1(Y^1, Y_{mp}^1)] \\ W^2 &= M[f^2(Y^2, Y_{mp}^2)] \end{aligned} \quad (2)$$

где M – знак математического ожидания; Y^{*2} – реальный результат применения системами своих управляющих воздействий; Y_{mp} – требуемый результат. Для двухстороннего антагонистического конфликта показатели эффективности однозначно связаны соотношениями:

$$W_{k+1}^1 = -W_{k+1}^2, \text{ и } W^1 = -W^2,$$

Необходимо синтезировать целевую структуру S_2 , удовлетворяющую условию:

$$W^2 = \min f \left(\frac{\left(\frac{Y_n - Y_d}{Y_d} \right)}{R} \right) \quad (3)$$

где W^2 – уровень эффективности системы S_2 ; Y_d – достигнутый результат функционирования СИБ КП после внедрения предложенных решений; Y_n – начальный результат функционирования СИБ КП; R – затраты на достижение данного результата. В соответствии с принятыми международными практиками, зададим R :

$$R : R = \text{const} \leq R_{\text{КП}} \times 0,3 \quad (4)$$

где $R_{\text{КП}}$ – стоимость внедрения и эксплуатации самого КП.

Применительно к СИБ КП в качестве достигнутого и начального результата функционирования наиболее целесообразно применение таких критериев, как, соответственно, достигнутый и начальный уровень уязвимости КП (УУ), которые могут использоваться и СИБ для оценки достигнутого уровня безопасности КП, и СНИБ для нарушения ИБ ресурсов КП. Целью S_2 является отсутствие уязвимостей КП или исключение возможности их использования СНИБ. При этом допускается наличие в КП уязвимостей, использование которых СНИБ не ведет к снижению уровня защищенности КП ниже требуемого.

Достигнутый УУ КП характеризуется конечным числом параметров, связанных с СИБ КП, к которым предъявляются следующие требования:

$$\begin{cases} Y_d^2 = \min_k \{Y_k(x_k, v_k)\} \leq Y_{mp} \\ Y_d^2 \rightarrow 0 \end{cases} \quad (5)$$

где x_k – характеристики и состояние средств защиты СИБ КП; v_k – характеристики управляющего воздействия; k – количество шагов взаимодействия, определяющееся сроком функционирования КП. Минимальное значение Y_d^2 будет достигнуто при одновременном выполнении следующих условий:

$$\begin{cases} X = \max f_1(p_{x0}, p_{x1}, p_{x2}, p_{x3}) \\ V = \max f_2(p_{v1}, p_{v2}, p_{v3}) \end{cases} \quad (6)$$

что означает такое состояние и характеристики СИБ, при которых обеспечивается минимальный УУ КП, где:

p_{x0} – показатель полноты множества угроз КП, которые СИБ может идентифицировать;

p_{x1} – показатель полноты множества угроз КП, которые СИБ может предотвратить;

p_{x2} – показатель управляемости процессов ИБ КП;

p_{x3} – показатель соответствия КП требованиям ИБ;

p_{v1} – показатель оперативности выявления и реагирования СИБ КП на выявленную угрозу;

p_{v2} – показатель полноты БД с информацией об угрозах нарушений ИБ КП;

p_{v3} – показатель полноты БД с информацией об уязвимостях КП.

Для учета важности каждого показателя экспертно зададим весовые коэффициенты для каждого показателя, в зависимости от его влияния на результат функционирования СИБ КП:

$$p_{x0} = 0,3; p_{x1} = 0,4; p_{x2} = 0,1; p_{x3} = 0,7; p_{v1} = 0,6; p_{v2} = 0,5; p_{v3} = 0,5.$$

На управляющее воздействие СИБ КП накладываются следующие ограничения, обязывающие СИБ КП реагировать на угрозы быстрее, чем СНИБ может адаптироваться к изменению средств защиты, а также быть более информированной, чем СНИБ:

$$\begin{cases} p_{v1}^2 \geq p_{v1}^1 \\ p_{v2}^2 \geq p_{v2}^1 \\ p_{v3}^2 \geq p_{v3}^1 \end{cases} \quad (7)$$

Таким образом, основная задача СИБ формулируется следующим образом – определить такие характеристики средств защиты СИБ КП, которые обеспечивают минимум интегральной целевой функции оценки уровня эффективности СИБ при достижении максимума функций $X = \max f_1$ и $V = \max f_2$ (6) и при заданных ограничениях на стоимость мер защиты (4) и на управляющие воздействия СИБ КП (7).

При этом, задача СИБ КП заключается в выработке такого управления, чтобы $W^2(v^*) > W_{mp}^2$ и $Z_{k+1}^2 = Z_k^2$, k – количество шагов взаимодействия систем.

Эффективность W_{mp}^2 соответствует условиям функционирования СИБ КП, при которых отсутствуют доступные для использования системой S_1 уязвимости КП либо возможно наличие уязвимостей,

использование которых системой S_1 будет приводить к нарушениям ИБ КП, ущербом от которых можно пренебречь.

Эффективность соответствует условиям функционирования СИБ КП, при которых отсутствуют доступные для использования системой S_1 уязвимости КП либо возможно наличие уязвимостей, использование которых системой S_1 будет приводить к нарушениям ИБ КП, ущербом от которых можно пренебречь.

Результаты анализа архитектуры и условий функционирования КП показывают, что внедрение КП несет в себе не только очевидные преимущества, но также добавляет новые угрозы нарушения ИБ всей организации. КП становится одним из наиболее критичных с точки зрения ИБ ИР в организации. Анализ угроз нарушения ИБ КП позволяет сделать вывод о необходимости применения дополнительных средств ИБ КП, позволяющих учитывать особенности технологий построения КП и условий их функционирования. Противодействие угрозам нарушения ИБ КП наиболее эффективно организовывать путем минимизации угроз и уязвимостей в компонентах КП и условиях функционирования, которые может использовать СНИБ для нарушения ИБ ресурсов КП. Ис-

пользование системами ИБ жестких, наперед заданных алгоритмов функционирования неэффективно. Более эффективный алгоритм поведения СИБ КП, в котором одновременно с реализацией КП в соответствии с предъявленными требованиями ИБ используются также адаптивные средства защиты.

ЛИТЕРАТУРА

1. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса / Под ред. д.т.н., проф. В.А. Минаева. – М.: Гелиос АРВ, 2002.
2. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. – М.: Статистика, 1980.
3. Михалевич В.С., Волкович В.Л. Вычислительные методы исследования и проектирования сложных систем. – М.: Наука, 1982.

Велигодский Сергей Сергеевич,

ОАО «Сбербанк России»,

e-mail: ssveligodsky@sberbank.ru

Филиппов Владимир Александрович,

канд. техн. наук, профессор МГИЭМ.

e-mail: filbob@infoline.su

А.Д. Калужский

КАТАЛОГИЗАЦИЯ ИЗДЕЛИЙ: ВОПРОСЫ СОПОСТАВИТЕЛЬНОГО АНАЛИЗА

В работе рассматривается вопрос возможного развития стандартов по каталогизации изделий. Обсуждается проблема применения результатов каталожного описания изделий для проведения их сопоставительного анализа. В качестве аппарата анализа предлагается метод дискретного измерения эффективности функционирования изделия, приводятся основные соотношения для расчета и соответствующая методика.

Ключевые слова: метод, измерение, решение, оборудование, эффективность, норма, системный подход, анализ, оценка

1. Введение

1.1. Общие положения. За последнее десятилетие был разработан и введен ряд стандартов, посвященных вопросам каталогизации изделий. В рамках этих стандартов были разработаны формы каталогизации, правила каталожного описания, уточнены тер-

A.D. Kaluzhskiy

CATALOGIZATION OF PRODUCTS: THE QUESTIONS OF THE COMPARATIVE ANALYSIS

In this article we review a problem of possible development of standards in catalogization of products. We discuss a question of application of products' catalogization description results to conduct benchmarking. As a method for analysis we offer the method of discrete measurement of effectiveness of product operation, also we give main correlations for calculation and appropriate technique.

Keywords: method, measurement, decision, equipment, effectiveness, standard, system approach, analysis, evaluation

мины и определения и т.д. [1-8]. Была проведена разработка единого кодификатора изделий [9], что позволяет провести их классификацию, создав тем самым ряд групп одинакового функционального назначения. Одновременно проводился процесс каталогизации большого числа систем и устройств раз-