КАЧЕСТВО ИННОВАЦИИ ОБРАЗОВАНИЕ

ISSN 1999-513X

№6
2011

журнал в журнале

КАЧЕСТВО и ИПИ (CALS)-технологии

www.quality-journal.ru

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

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),
nii@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. Краснобогатырская, д. 6., www.sts-print.ru

Журнал входит в перечень ВАК РФ

Статьи рецензируются

КАЧЕСТВО ИННОВАЦИИ ОБРАЗОВАНИЕ

Номер 6 (73), июнь, 2011

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

Сведения о членах редколлегии и об авторах статей можно найти на сайте журнала www.quality-journal.ru

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 зашиты. 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

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

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 позиций 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 портальный 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 портального решения, неправиль-

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

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

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

где Z_k^1 – траектория процесса смены состояний S_1 до момента t_{k+1}, $Z_k^1 = \left\{z_0, z_1, ..., z_k\right\}$; Z_k^2 – траектория процесса смены состояний S_2 до момента t_{k+1}, $Z_2^k = \left\{z_0, z_1, ..., z_k\right\}$; u^k, v^k – совокупность управляющих воздействий систем S_1 и S_2 соответственно до момента t_{k+1}, $u^k = \left\{u_0, u_1, ..., u_k\right\}, u^k \in U$, $v^k = \left\{v_0, v_1, ..., v_k\right\}, v^k \in V$, U, V – множества возможных взаимных воздействий систем S_1 и S_2 соответственно; Z_{ucx}^1, Z_{ucx}^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:

$$u = \left\{u^0, u^1, ..., u^k\right\},$$
$$v = \left\{u^0, u^1, ..., u^k\right\}.$$

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^{12} реального результата, достигнутого системой к оцениваемому моменту времени:

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

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

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

Необходимо синтезировать целевую структуру S_2, удовлетворяющую условию;

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

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

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

где $R_{КП}$ – 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:

$$\begin{cases} Y_Д{}^2 = \min_k \{Y_k(x_k, v_k)\} \le Y_{тр} \\ Y_Д{}^2 \to 0 \end{cases} \quad (5)$$

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 $Y_Д{}^2$ 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:

$$\begin{aligned} p_{v1}{}^2 &\ge p_{v1}{}^1, \\ p_{v2}{}^2 &\ge p_{v2}{}^1, \\ p_{v3}{}^2 &\ge p_{v3}{}^1 \end{aligned} \quad (7)$$

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 $W^2(v^*) > W^2_{тр}$ и $Z^2_{k+1} = Z^2_k$, k - количество шагов взаимодействия систем.

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