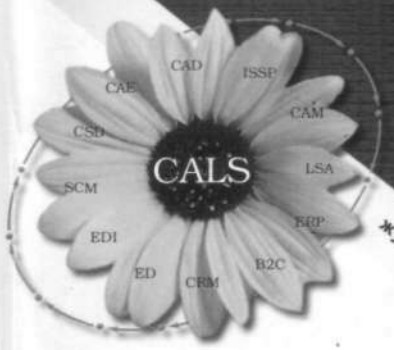
КАЧЕСТВО ИННОВАЦИИ ОБРАЗОВАНИЕ

ISSN 1999-513X

№7
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 7 (74), июль, 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

(изучено 100 источников), позволил, во-первых, расширить представление об области применяемых методов (факторный, регрессионный анализ), что даст возможность многие задачи решать более эффективными способами, и, во-вторых, выявил новые методы, которые не удалось обнаружить при систематическом обзоре публикаций из области медицины и психологии, несмотря на несомненную их перспективность в данной сфере:

1. Кластерный анализ.
2. Многомерное шкалирование.
3. Метод нейронных сетей.

Выявленные методы также можно считать чрезвычайно важными для повышения качества медицинских и психологических исследований.

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России», Государственный контракт № П946 от 20.08.2009 г.

Воробьёв Андрей Викторович,
канд. психологич. наук, ст. науч. сотр.
Московский Государственный Индустриальный Университет.
e-mail: aworobiev@mail.ru.
Колемасов Иван Сергеевич,
науч. сотрудник, МГИУ
e-mail: kolemasoff.
Финагин Василий Геннадьевич,
науч, сотрудник, МГИУ,
e-mail: myseries@mail.ru.

С.С. Велигодский, В.А. Филиппов

МОДЕЛЬ И АЛГОРИТМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ПОРТАЛОВ

Рассмотрена общая модель противодействия угрозам нарушения информационной безопасности корпоративных порталов. Сформулирован общий алгоритм поведения системы информационной безопасности КП. Разработан детализированный алгоритм функционирования системы зашиты, основанный на двухуровневой адаптации – параметрической и дискретной, а также наполнение стратегий защиты.

Ключевые слова: информационная безопасность, системы зашиты, корпоративные порталы

S.S. Veligodsky, V.A. Filippov

MODELS AND ALGORITHMS OF COUNTERACTION AGAINST INFORMATION SECURITY THREATS OF ENTERPRISE PORTALS

The general model of counteraction against information security threats of enterprise portals is considered. The general algorithm of behavior of information security system is formulated. The detailed algorithm of security system functioning, based on two-level adaptation - parametrical and discrete, and security strategies filling are developed.

Keywords: information security, enterprise portals, security threats, interaction model, vulnerability, algorithm of interaction, security models

Противодействие угрозам нарушения информационной безопасности (ИБ) требует формирования модели конфликтного взаимодействия средств нарушения ИБ (СНИБ) и системы обеспечения ИБ (СОИБ) корпоративных порталов (КП). Структурно общая модель взаимодействия СНИБ и СОИБ КП может быть построена на общей конфликтной модели взаимодействия и должна состоять из совокупности взаимосвязанных блоков (рис. 1).

Система S_1 – СНИБ КП, система S_2 – СОИБ КП. Индексы «1» и «2» указывают на систему S_1 и S_2 соответственно. Блок *1* отображает процесс смены состояний системы (Z_1^k, Z_2^k) и достигнутый результат (Y_k^1, Y_k^2) применения управляющих воздействий, который подается в блок *2* для оценки (W_k^1, W^1, W_k^2, W^2) их эффективности. По результатам оценки эффективности в блоке *3* (центре управления $S^*_{1,2}$), обладающем необходимыми правилами и компетенциями, вырабатывается внутреннее управление по выбору наиболее оптимального образа действий. Управляющие воздействия (u^k, v^k) вырабатываются в блоке *4* на основе управлений блока *3* и наличия и состояния средств защиты (R_0^1, R_0^2), отображенных блоком *5*. Для учета условий протекания взаимодействия в состав модели включен блок *6*, отображающий воздействие условий функционирования КП.

Средства защиты (активные средства воздействия и защитные средства противодействия) представля-

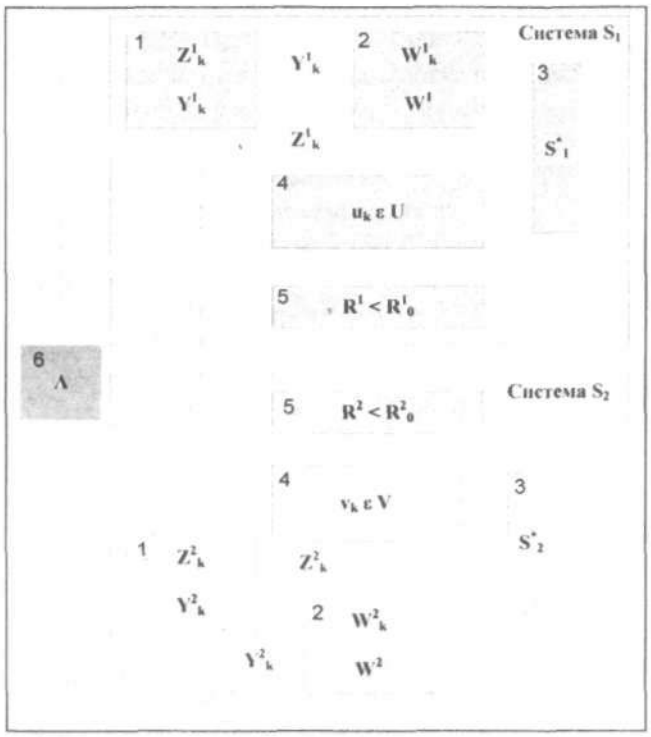


Рис. 1. Модель взаимодействия СНИБ и СОИБ КП

ются техническими характеристиками и совокупностью ресурсов. На каждый вид ресурсов накладываются ограничения:

$R^1_d \quad R^1_{d0}, \; d=1(1)D,$

$R^2_m \quad R^2_{m0}, \; m=1(1)M,$

где d, m – номера видов ресурсов сторон S_1, S_2 соответственно; R^1_{d0}, R^2_{m0} – запас ресурсов d-го, m-го видов соответственно.

При этом управляющие воздействия в блоке *3* СОИБ КП должны быть такими, что при смене состояний $Z^k_2 \to Z^{k+1}_2$ результат применения управляющих воздействий v_k не должен приводить к ухудшению уровня защиты $Y^2_k \le Y^2_{k+1}$.

Такая структура модели конфликтного взаимодействия систем позволяет синтезировать функциональные подсистемы, составляющие СОИБ КП, последовательность управляющих воздействий, описывающую адаптивное поведение S_2 (СОИБ КП) и удовлетворяющую заданным условиям.

Общий алгоритм функционирования СОИБ КП может быть представлен следующим образом (рис. 2).

Здесь $УУ_i$ – уровень уязвимости (УУ), достигнутый на i-ом шаге; $УУ_д$ – допустимый УУ; R_i – ресурсы, затраченные СОИБ на i-ом шаге. $R_д$ – допустимое количество ресурсов, которое может использовать СОИБ.

Также данный алгоритм может быть представлен следующим образом в виде логического описания:

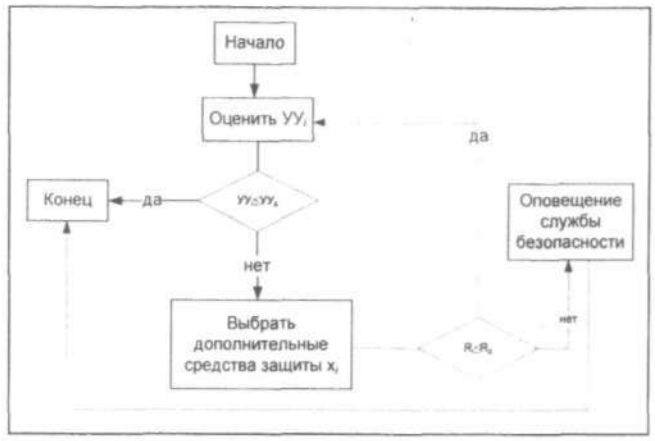


Рис. 2. Общий алгоритм функционирования СОИБ КП

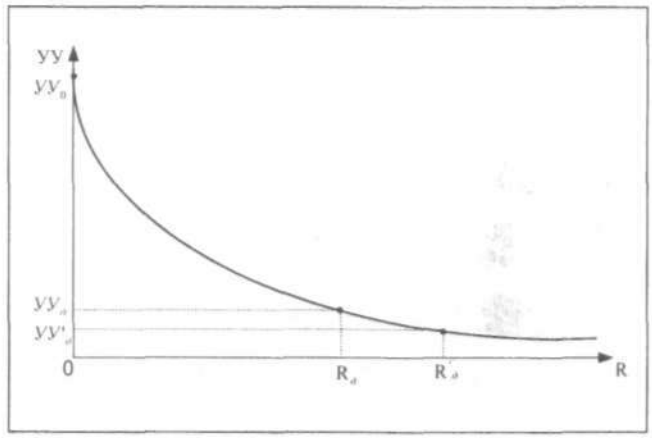


Рис. 3. График зависимости УУ и стоимости защитных мер

Делать:

Оценка $УУ_i$

Если $УУ_i \ge УУ_д$ *то используем* x_i *со стоимостью* $\sum_{i=0}^{i-1} R_i \le R_д$

Пока не:

$$\sum_{i=0}^{i-1} R_i > R_д \text{ или } УУ_i < УУ_д$$

Если:

$\sum_{i=0}^{i-1} R_i > R_д$, *то оповестить службу безопасности о необходимости добавления ресурсов.*

Графически результат работы модели может быть представлен в виде графика зависимости УУ от затраченных ресурсов СОИБ на снижение (**Ошибка! Источник ссылки не найден.**). Предполагается, что начальный УУ ($УУ_0$) является высоким, и при применении защитных мер он начинает постепенно снижаться, пока не достигнет некоторого уровня, где

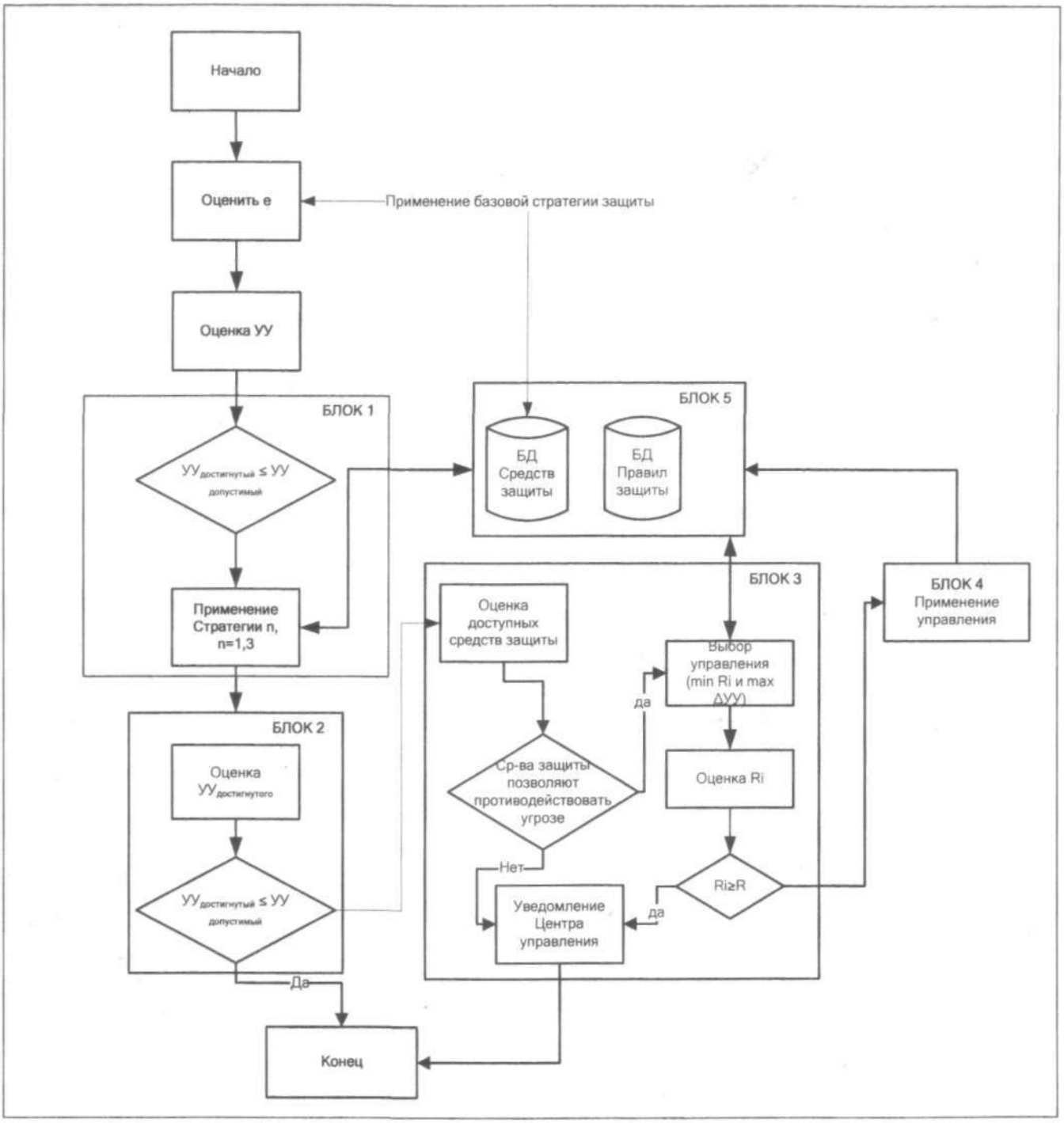


Рис. 4. Развернутый алгоритм функционирования СОИБ КП

дальнейшее наращивание ресурсов СОИБ уже не будет оказывать на него воздействия.

В практических задачах взаимодействие СНИБ и СОИБ КП при наличии ограничений на ресурсы СОИБ будет осуществляться либо до достижения предела заданных ресурсов ($R_д$), которому соответствует условно допустимый УУ ($УУ'_д$), либо при достижении приемлемого УУ ($УУ_д$), затратив часть выделенных ресурсов ($R'_д$).

На рис. 4 представлен развернутый алгоритм функционирования СОИБ КП. На данном рисунке выделены элементы СОИБ и связи между ними, разработанные в рамках настоящей работы.

Применение средств защиты в СОИБ КП основано на стратегиях защиты (рис. 5): *Стратегия 1* – использование только базового уровня защиты; *Стратегия 2* – активация адаптивных средств СОИБ КП (СВУ, САЗ, МЭ), *Стратегия 3* – усиление СОИБ

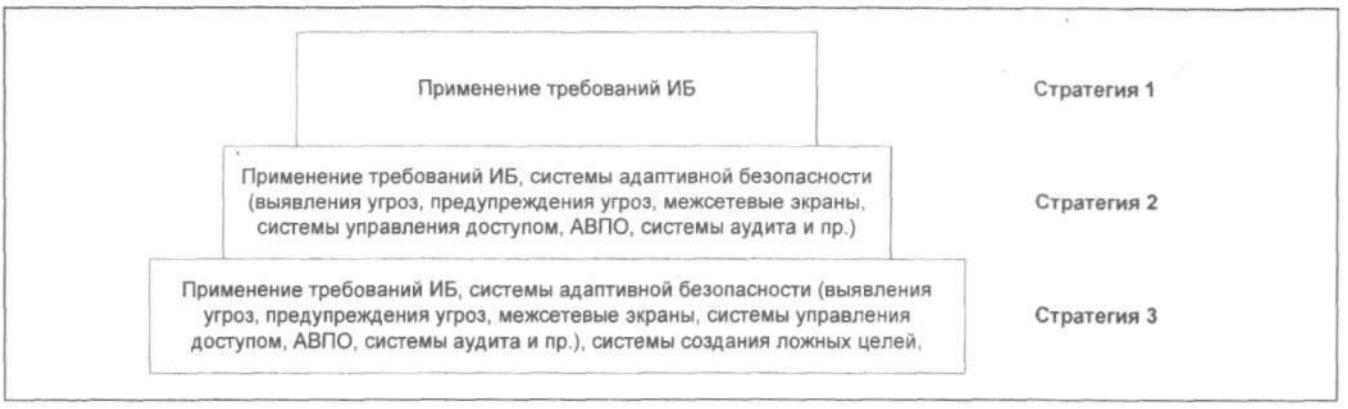


Рис. 5. Стратегии защиты в СОИБ КП

ССЛЦ, повышение управляемости СОИБ, повышение показателей СОИБ. Дальнейшие шаги по снижению УУ КП приводят к необходимости расходования значимых ресурсов фактически при сохранении УУ и в подавляющем большинстве случаев являются экономически не оправданными.

Стратегия 3, используя максимальное количество ресурсов, позволяет существенно снизить УУ ИР КП. В данной стратегии одновременно с адаптивными средствами защиты предусматривается применение встроенных средств защиты КП, организованных в соответствии с требованиями информационной безопасности. В случае, если встроенные средства защиты не позволяют выявить и предотвратить угрозу, автоматически активируются дополнительные адаптивные средства. При этом в составе адаптивных средств функционирует специализированная маскирующая система, в задачи которой входит скрытие ИР КП в случае выявления угрозы и создание сигнатурных описаний уязвимостей для обновления БД средств защиты. Схематично подход к защите на базе стратегий может быть представлен рис. 5.

Для любой из стратегий является критичным обеспечить отсутствие катастрофических и критических уязвимостей и снизить УУ до допустимого уровня, что предполагает при невыполнении условия $УУ_i < УУ_д$ применение дополнительных средств защиты, доступных в рамках стратегии, и, возможно, переход в другую стратегию защиты, но в рамках ресурсных ограничений.

Для учета начальной ситуации в алгоритме присутствует блок, обеспечивающий учет текущей стоимости ИР КП для выбора начальной стратегии защиты. В блоке используется критерий e, оцениваемый следующим образом:

$$e = \frac{R_{кп} - R_{ир}}{R_{кп}},$$

где, $R_{кп}$ – стоимость всех компонент КП, включая стоимость его ИР; $R_{ир}$ – стоимость защищаемых ИР КП.

Базовая стратегия выбирается исходя из следующих соотношений:

1) e 0,3 – стратегия 1;
2) 0,3> e 0,7 – стратегия 2;
3) e >0,7 – стратегия 3.

Таким образом, чем больше стоимость ресурсов, КП, тем более ресурсоемкая стратегия защиты может применяться изначально в качестве базовой.

Алгоритм функционирования СОИБ КП предполагает, что в случае, если угроза преодолевает средства защиты базовой стратегии, ее обнаруживают и ликвидируют дополнительные средства СОИБ КП. При этом традиционный адаптивный подход, в котором применяются средства выявления и предотвращения угроз, усилен, и в него добавлены маскирующие компоненты, функционирующие в среде Веб-приложений. Таким образом, если СОИБ КП не может предотвратить угрозу, включаются средства маскировки ИР КП, позволяющие существенно затруднить для СНИБ возможность воздействия на ИР КП. При этом для СОИБ КП наибольшая эффективность достигается при реализации алгоритмов поведения, синтезируемых по правилам гибкого реагирования и активного поведения, при этом: $W^2(v_{an}) > W^2(v_{zp})$, то есть в рамках поставленной задачи наибольшую эффективность имеет стратегия активного поведения.

Велигодский Сергей Сергеевич,
ОАО «Сбербанк России»,
e-mail: ssveligodsky@sberbank.ru

Филиппов Владимир Александрович,
канд. техн. наук, профессор, МГИЭМ.
e-mail: filbob@infoline.su