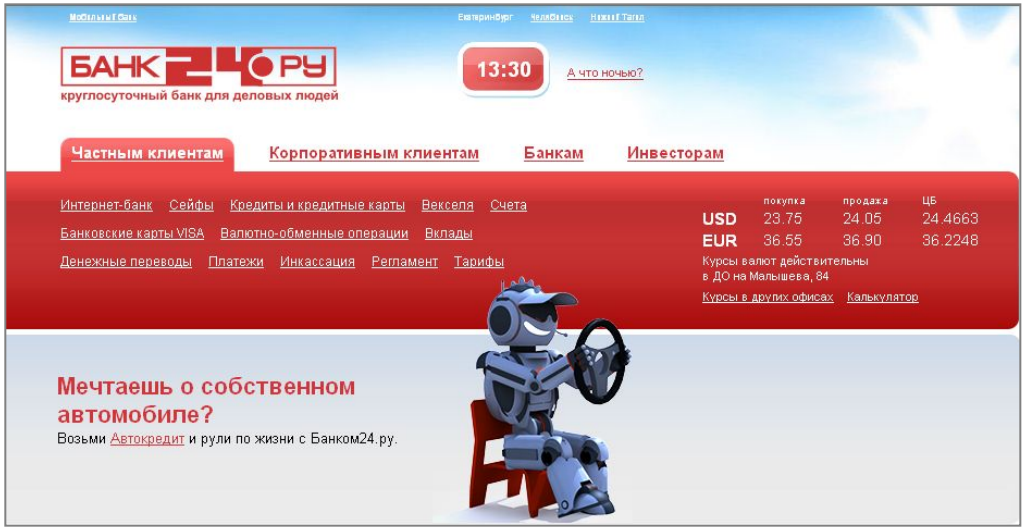
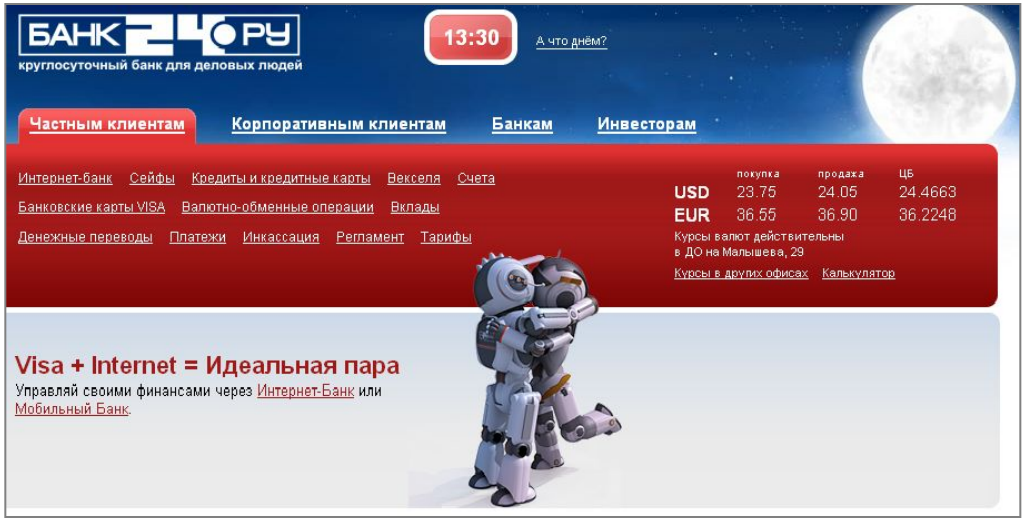
БАНК 24 РУ
круглосуточный банк для деловых людей

Системное управление рисками информационной безопасности на основе ISO 27001:2005

Валентин Никонов, к.э.н., PMP IPMA, QMS Auditor
Советник председателя Совета Директоров «Банк24.ру» (ОАО)

«Банк24.ру» - первый Банк в России





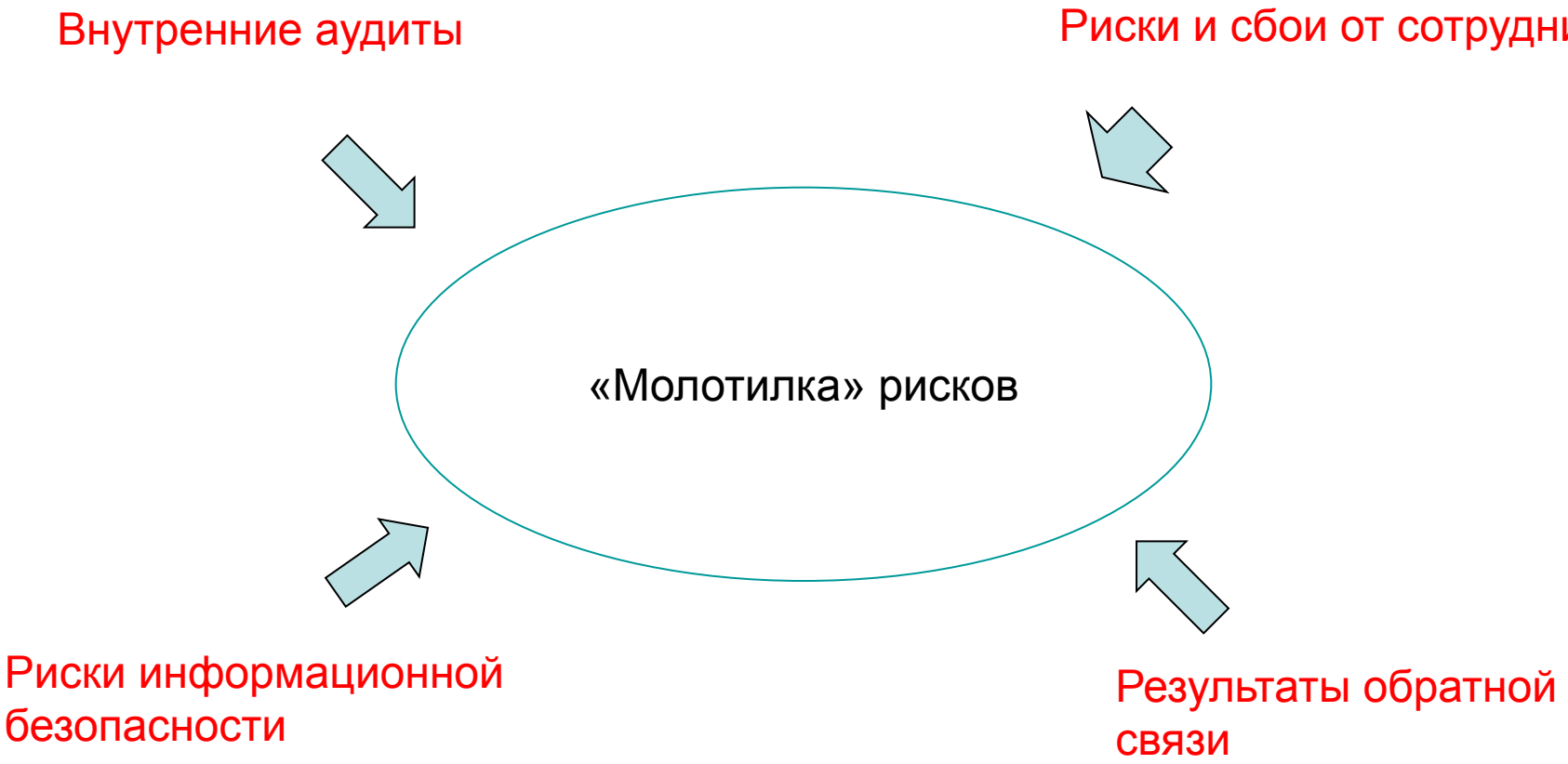
Принципы

- Системные решения
- Подходы риск-менеджмента
- Интеграция в общую систему управления операционным риском
- Корпоративная культура

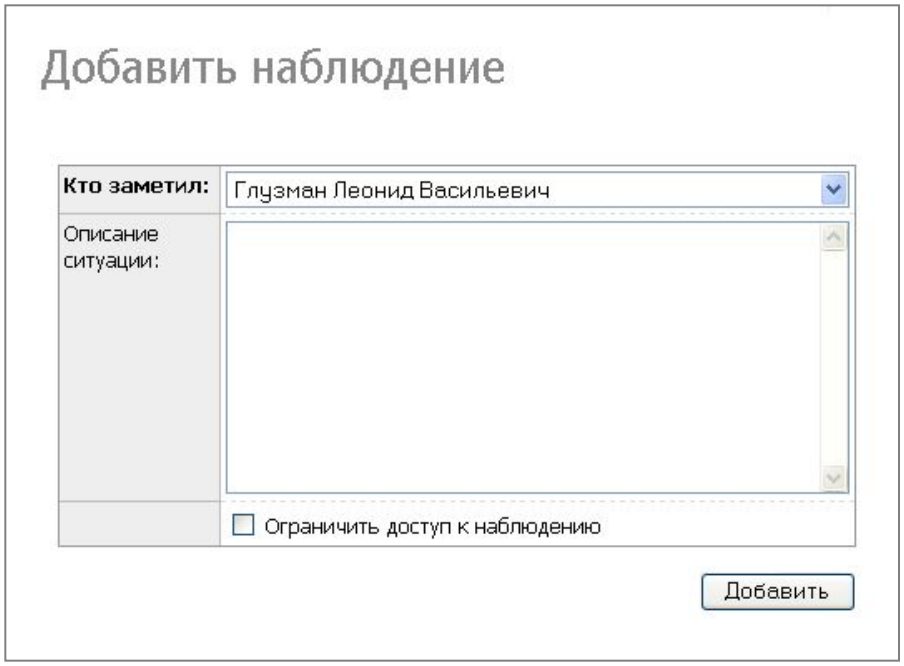
Интегрированная система менеджмента

- ISO 9001:2000 базовый стандарт на систему управления (система управления процессами)(2004)
- Система управления проектами (2004 – на основе модели Organizational Project Management Maturity Model)
- Система менеджмента информационной безопасности (ISO 27001:2005)
- Система управления операционным риском (ISO 9001)
- Система корпоративного управления (IFC standards)

Подходы риск-менеджмента



Обработка рисков

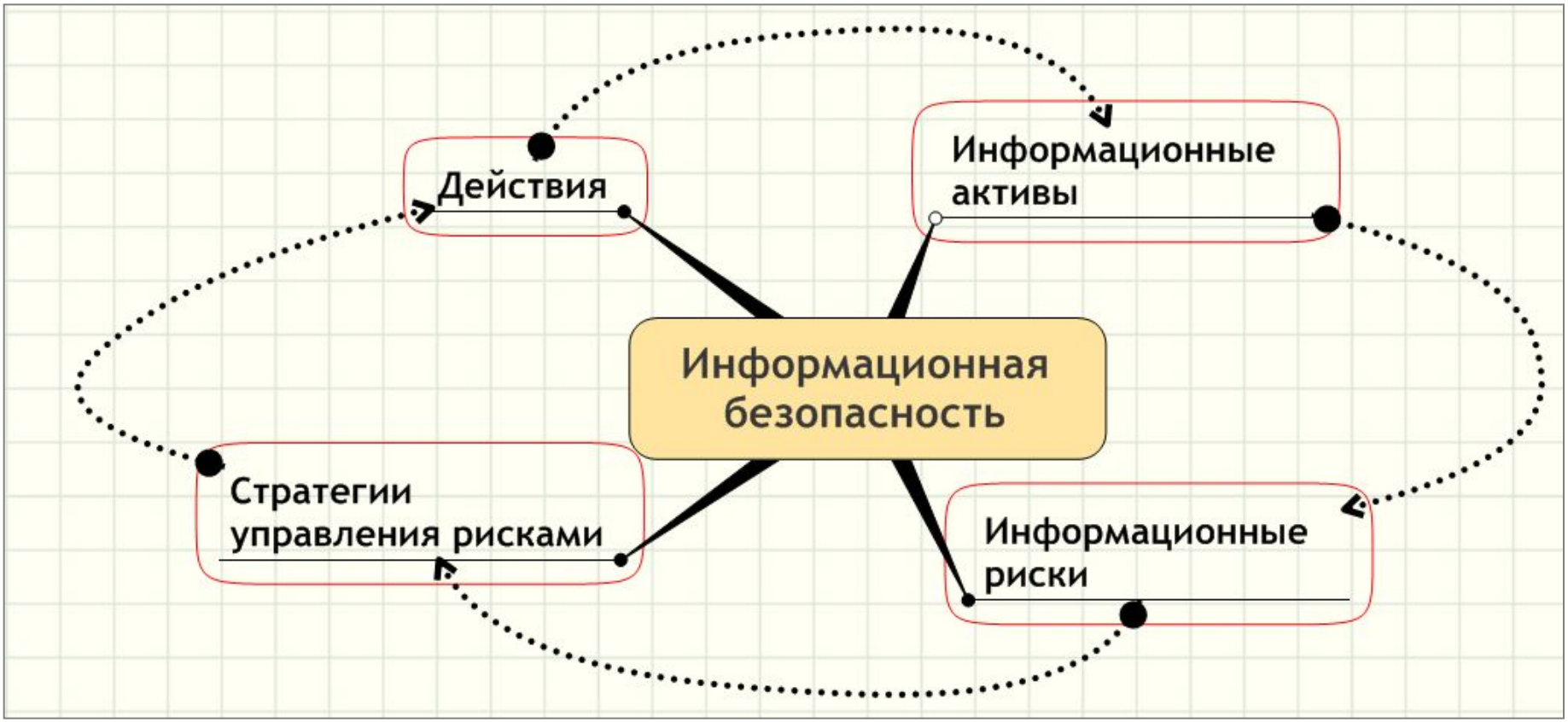


Наблюдение	№ **2184** от **18.02.08**	Состояние:	**В работе**		Подробно
Описание:	При обмене валюты выдается справка. В этой справке в конце листа расположена рекламная информация по вкладу "Альфа-Ромео" которого уже давно нет. Там же написано, что можно выиграть новый автомобиль Альфа-Ромео! Такая акция была очень-очень давно!				
Подразделение:	Отдел маркетинга				
Документы:					
Инициатор:	Прошко Е.Д.				
Руководитель РГ:	Голубева О.И.	Дата анализа:	27.02.08	Дата закрытия (план):	10.03.08
Аудитор:	Кузьменко С.В.			Дата закрытия (факт):	Нет

ISO 27001:2005

- Международный стандарт на систему менеджмента информационной безопасности
- Выпущен ISO в 2005 году
- Обеспечение «необходимой и достаточной информационной безопасности»
- Подходы риск-менеджмента

Логика системы



Политика системы

УТВЕРЖДЕНО
Решением Совета директоров
«Банк24.ру» (ОАО)
Протокол от «__»_____2007г.
№_____

ПОЛИТИКА № 231/3 от 22.09.2006

ПОЛИТИКА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ "БАНК24.РУ" (ОАО)

Статус: Утверждено

Версия: 2.0 от

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Цель

Цель Политики системы управления информационной безопасностью: обеспечить выполнение целей, указанных в Политике обеспечения информационной безопасности, в точном соответствии с требованиями ИСО 27001 в области применения стандарта в Банке.

Политика системы управления информационной безопасностью является подполитикой Политики обеспечения информационной безопасности и конкретизирует ее в области применения СУИБ.

1.2. Термины, определения и соглашения

Термин	Определение, толкование
Банк	«Банк24.ру» (ОАО)
Информационные активы	Любые данные, информация, имеющие ценность для Банка, а также активы, прямо или косвенно оказывающие влияние на информацию на всех стадиях ее жизненного цикла (программное обеспечение, оборудование, персонал и т.д.).
Информация	Сведения (сообщения, данные) независимо от формы их представления
Угроза информации	Потенциально возможное событие (действие), могущее нанести вред информации.
Защита информации	Комплекс мероприятий (организационных, технических, технологических), проводимых с целью предотвращения (снижения вероятности) реализации угроз информации.
Информационная безопасность	Обеспечение конфиденциальности, целостности и доступности информации, а также подлинности информации и надежности систем.
Доступность информации	Свойство быть доступным и используемым со стороны авторизованной стороны

Что защищать?

- Информационные активы
  - Конфидецниальность
  - Целостность
  - Доступность
- Базы данных, серверы, компьютеры и т.д.

Управление информационными активами

Порядок № 234/2 от 29.09.2006

Порядок управления реестром информационных активов

Статус: Утверждено
Версия: 1.0 от 29.09.2006

	Должность	Ф.И.О.	Подпись	Дата
Утверждено:	Председатель Правления	Лапшин С.Г.		29.09.2006
Разработал:	Администратор информационной безопасности	Нахимов В.П.		25.09.2006
Согласовано:	Начальник Службы безопасности	Пенкин Н.П.		26.09.2006
Согласовано:	Начальник Управления информационных технологий	Карфидов И.А.		26.09.2006
Согласовано:	Начальник Хозяйственно-эксплуатационного управления	Ахметов В.З.		27.09.2006
Согласовано:	Начальник Расчетного центра	Калиниченко Н.А.		27.09.2006
Согласовано:	Начальник Отдела маркетинга	Кузименко С.В.		27.09.2006
Согласовано:	Начальник Управления розничного бизнеса	Нагимова Н.П.		28.09.2006
Согласовано:	Начальник Кредитного отдела	Приценко О.Ю.		29.09.2006
Согласовано:	Заместитель Директора Казначейства	Швецова М.В.		29.09.2006
Согласовано:	Начальник Юридического отдела	Морозова Ю.А.		27.09.2006
Согласовано:	Заместитель главного бухгалтера	Яцына С.Д.		28.09.2006
Согласовано:	Начальник Отдела анализа и контроля рисков	Осинкина Н.Г.		28.09.2006
Согласовано:	Ведущий специалист Общего отдела	Сорокина Ю.Н.		29.09.2006
Согласовано:	Исполнительный директор	Дьяконов Б.П.		28.09.2006

Процедура управления информационными рисками

УТВЕРЖДЕНО
Председатель Правления
«Банк24.ру» (ОАО)

_____С.Г.Лапшин

« » марта 2008г.

Порядок № 234/1 от 29.09.2006 г.

Порядок управления информационными рисками

Статус: Утверждено
Версия: 4 от

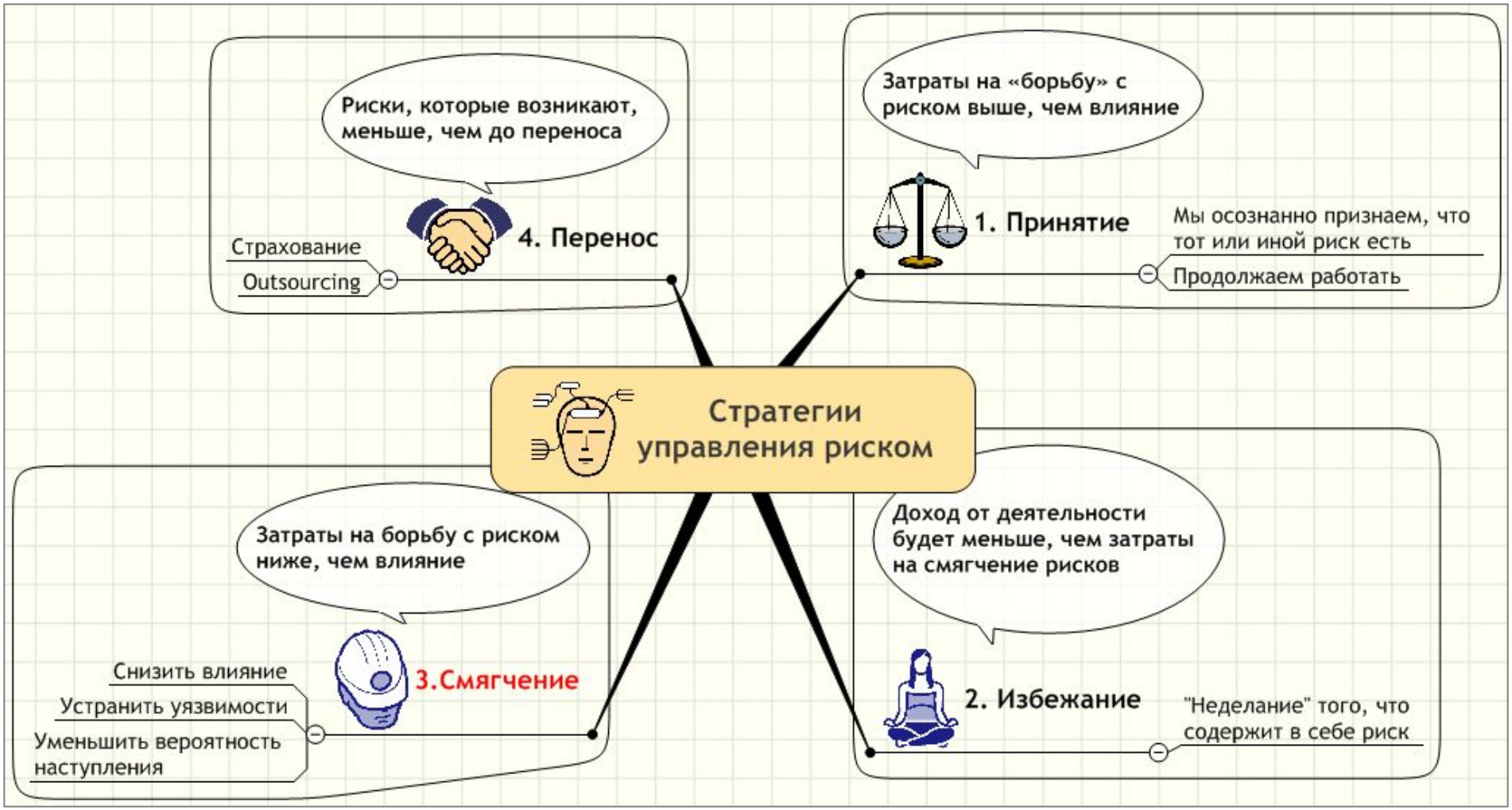
СОДЕРЖАНИЕ

Риски информационной безопасности

Ключевые процедуры

- Реестр информационных активов
- Профиль рисков информационной безопасности

Стратегии управления рисками



Положение о применимости контролей

УТВЕРЖДЕНО
Решением Правления
«Банк24.ру» (ОАО)
Протокол от « 19» февраля 2008г.
№ П- 19/02

ПОЛОЖЕНИЕ № 90/1 от 19.02.2008

Положение о Применимости Контролей (SoA)

Статус: Утверждено
Версия: 1.0 от 19.02.2008

СОДЕРЖАНИЕ

Контроли (смягчение рисков)

- Information Security Policy
- IT support procedure
- Software development, implementation and modification requests management
- Asset Inventory Management Procedure
- Procedures for protection of confidential information (information of limited access)
- Use of informational assets and recourses

Контроли (смягчение рисков)

- Instruction for personnel employment
- Physical Security Procedure
- Procedures for back-up
- Software development
- Procedures for antivirus management
- Removable media management procedure
- Information Security implementation in the ‘Internet Bank for private clients’ service provision

Концепция применения международных стандартов

SPECIAL REPORT

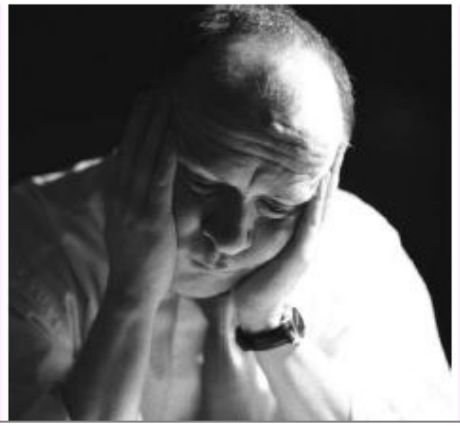
CONTINUITY AND RISK

Applying ISO management system standards to enterprise risk management

ISO management system standards can be important tools in a company-wide risk management programme. The first step is to understand what is meant by a generic risk management system. Next, the organization needs to look at how a standards-based system can be implemented.

by Valentin Nikonov

Valentin Nikonov is a project management professional recognized by the International Project Management Association and a certified ISO 9001:2000 auditor. As a senior specialist with the Growth Trajectory consultancy, located in Yekaterinburg, Russia, he is responsible for projects to implement integrated management systems, including risk management systems. Mr. Nikonov also participates in the activities of working party WP.6 of the United Nations Economic Commission for Europe.



For decades, ISO management system standards have proved invaluable to organizations around the globe aiming for improvement in a variety of areas: quality (ISO 9001:2000), information security (ISO/IEC 27001:2005), environment (ISO 14001:2004) and others.

These areas are quite specific and so are the standards. At the same time, there is an important unifier: they all can "work" for common goals – helping organizations of any type to systematically manage risks. That, in turn, is a condition for business stability, profitability and safety.

Результат

- Система процессов
- Систематическое управление рисками информационной безопасности (есть перечень стандартных мер)
- Устойчивый, бесперебойный, развивающийся бизнес