# Раздел III. Защита объектов информатизации

УДК 004.056.5, 004.89

**А.М. Цыбулин**

## МНОГОАГЕНТНЫЙ ПОДХОД К ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

*Процесс управления информационной безопасностью предприятия достаточно сложный и трудоемкий, особенно для распределенных гетерогенных информационных систем. Актуальной проблемой является автоматизация процесса управления.*

*Предлагается подход к построению автоматизированной системы управления информационной безопасностью предприятия на базе концепции многоагентных систем и процессного подхода к управлению. Под управлением понимается процесс воздействия на систему защиты информации с целью поддержания заданного или перевода её в новое состояние с другим, более низким уровнем относительного информационного риска.*

*Бизнес-процесс, интеллектуальный агент; многоагентная система; информационная безопасность; механизм защиты информации; управление информационной безопасностью; мониторинг; аудит; информационная система.*

**A.M. Tsybulin**

## MULTI-AGENT APPROACH TO THE DEVELOPMENT OF THE AUTOMATED MANAGEMENT SYSTEM OF ENTERPRISE'S INFORMATION SECURITY

*Process of enterprise's information security management is rather difficult and complicated, especially for allocated heterogeneous information systems. Automation of management process is an urgent problem.*

*Approach to the development of the automated management system of enterprise's information security based on multi-agent system concept and process approach to management has been suggested. Management is a process of influencing the information protection system for defined state or transferring the system to new state lower relative risk.*

*Business process; intelligent agent; multi-agent system, information security; information security management; monitoring, audit; mechanism of protection of the information; disaster tolerance; information system.*

Темпы развития информационных технологий, возрастающая сложность информационных систем (ИС) обуславливают необходимость повышения уровня интеллектуализации инструментальных средств исследования, и обеспечения информационной безопасности (ИБ) предприятия.

Эффективное функционирование предприятия достигается наличием постоянного доступа к точной и полной информации. Уровень ИБ должен всегда соответствовать этому принципу. Продукты и услуги, создаваемые предприятием должны быть качественными и доступны рынку или обществу, и нужны для выполнения определенных задач. Неадекватное информационное обеспечение влечет производство некачественных продуктов и услуг, которые не могут использоваться для выполнения соответствующих задач и ставят под угрозу существование организации

или безопасность зависящих от нее процессов. Процесс управления информационной безопасностью тесно связи с другими процессами управления, так как в них выполняются действия, связанные и с обеспечением ИБ. Эта деятельность проводится в обычном порядке в рамках ответственности определенного процесса. При этом процесс управления информационной безопасностью обеспечивает другие процессы инструкциями о структуре деятельности, связанной с ИБ.

Результаты анализа показывают, что процесс управления информационной безопасностью ИС предприятия достаточно сложный и трудоемкий, особенно для распределенных гетерогенных ИС. Актуальной проблемой является автоматизация процесса управления.

Предлагается подход к построению автоматизированной системы управления информационной безопасностью предприятия на базе концепции многоагентных систем и процессного подхода к управлению.

В автоматизированной системе используется потенциальная цель управления – это желаемый уровень защиты информации достижимый в принципе в перспективе, но в силу неопределенности планируемый с некоторой степенью вероятности. В качестве уровня защиты информации применяется относительный остаточный эндогенный риск.

Для защиты данных в ИС создаются и включаются в ее состав множества механизмов защиты, средств инвентаризации, мониторинга и аудита, которые образуют систему защиты информации.

Пусть множество механизмов защиты (МЗ):

$$\text{МЗ} = \{s_i\}, \quad (1)$$

где $s_i$ – $i$-й МЗ, $i=1,\ldots n$, $n$ – количество механизмов защиты в системе защите информации (СЗИ). Каждый$s_i$ характеризуется набором свойств (режимов работы), $П_{i1}$, $П_{i2}$, …, $П_{ir}$, которые можно выбирать при инициализации и/или изменять в процессе работы. Формальная модель каждого МЗ – это интеллектуальный агент $s_i$.

Совокупность всех $r$ – свойств $s_i$ называется состоянием $П_i$

$$П_i=\{П_{i1}, П_{i2}, \ldots, П_{ir}\}. \quad (2)$$

Каждое $j$ – состояние обеспечивает определенное значение относительного риска [1]:

$$\psi_{ij} = ((1-P_{ij}) * C_i / C^{\Sigma}{}_i), \quad (3)$$

где – $\psi_{ij}$ относительный риск $s_i$ – МЗ (агента); $C_i$ – ценность защищаемых информационных ресурсов $s_i$ – МЗ; $(1-P_{ij})$– вероятность реализации угроз информационной системе через $s_i$ – МЗ, который находится в $j$-м состоянии ($j=1,\ldots,r$); $C^{\Sigma}{}_i$ – суммарный неприемлемый ущерб. Отношение $C_i / C^{\Sigma}{}_i$ – коэффициент опасности угроз ИС через $s_i$ – МЗ.

Современные тенденции таковы, что в эксплуатации находится большое количество разнородных МЗ и в связи с этим возрастают вероятности ошибок в их конфигурации.

Под управлением понимается процесс воздействия на СЗИ с целью поддержания заданного или перевода её в новое состояние с другим уровнем относительного информационного риска.

По аналогии с классической структурой, структура автоматизированной системы управления информационной безопасности предприятия имеет вид, представленный на рис. 1.

Как любая система управления, она включает следующие основные процессы и блоки:

- $X(t)$ – входные бизнес-процессы *ИС*;

- *A(t)* – возмущающие процессы – воздействия атак внешних и внутренних злоумышленников на входные и основные бизнес-процессы, а информационные ресурсы *ИС* и т.д.;
- функциональный объект – это объект, в котором реализуются основные бизнес-процессы *ИС,* располагаются основные информационные ресурсы, базы данных и агенты мониторинга;

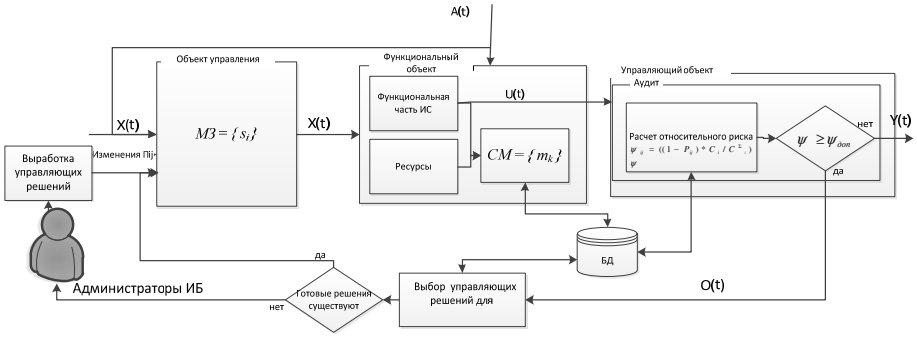


*Рис. 1. Система автоматизированного управления ИБ*

- управляющий объект – объект, в котором вырабатываются управляющие решения. В процессе аудита проводится анализ результатов работы агентов мониторинга, хранящихся в базе данных. Агент-аудитор рассчитывает текущий уровень относительного информационного риска и сравнивает его с требуемым уровнем, и в случае необходимости инициирует обратную связь;
- *O(t)* – обратная связь, которая включается в том случае, если вычисленное интеллектуальными агентами аудита значение относительного риска больше допустимого ($\psi \geq \psi_{доп}$);
- объект управления – это *i-го МЗ, i=1,…,n.* Управление заключается в смене состояний $П_i=\{П_{i1}, П_{i2}, …, П_{ir}\}$ *i-го МЗ.* Процесс управления реализуется интеллектуальными агентами управления, на основе выбора управляющих решений из базы данных;
- *U(t)* – основные бизнес-процессы *ИС*;
- *У(t)* – основные выходные бизнес-процессы ИС, в том числе и бизнес – процессы, обеспечивающие конфиденциальность, доступность и целостность информации, эффективность, которых оценивается интеллектуальными агентами значением относительного риска $\psi$. IDEF-диаграмма бизнес-процесса построения многоагентной системы приведена на рис. 2.

Очевидно, что именно система управления организации имеет возможность адекватно реагировать на внешние и внутренние воздействия, что придаёт организации способность к адаптации в изменяющихся условиях, делает её саморегулируемой.

Во многих МЗ, в операционных системах и системах управления базами данных имеются средства мониторинга определенных классов событий, среди них имеются события, которые позволяют выявлять инциденты безопасности. В состав средства мониторинга включаются и средства инвентаризации.

Множество средств мониторинга:

$$CM = \{ m_k \}, \quad (4)$$

где $m_k$ – k-ое СМ, k=1,…K,K – количество средств мониторинга в СЗИ. Формальная модель каждого СМ – это интеллектуальный агент $m_k$ [2, 3].

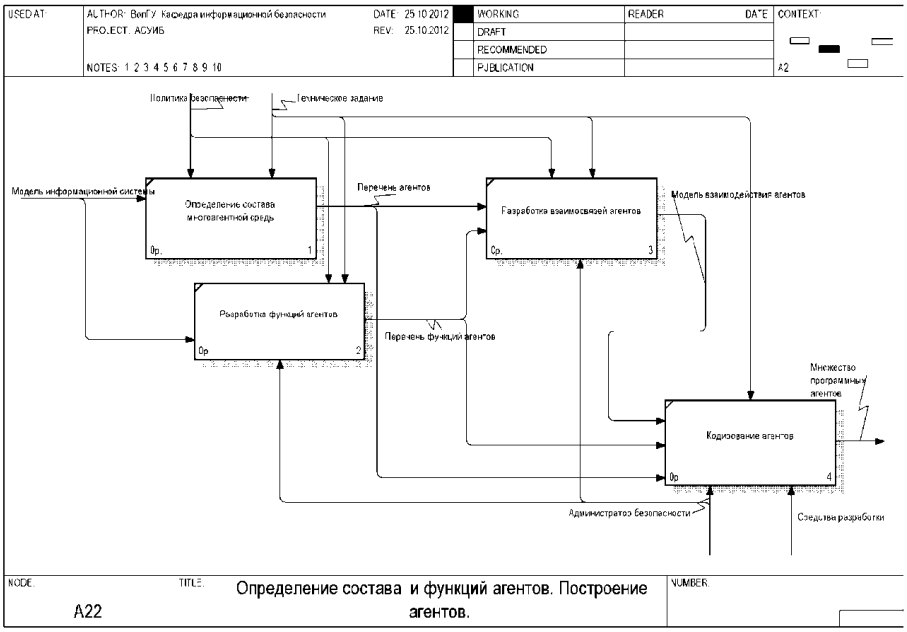


*Рис. 2. IDEF-диаграмма бизнес построения многоагентной системы*

Каждое $m_k$ характеризуется набором регистрируемых параметров, $M_{i1}$,$M_{i2}$, …, $M_{iK}$, которые можно выбирать при инициализации и/или изменять в процессе работы.

Мониторинг проводится как на сетевом, так и на системном уровне. Агенты сетевого мониторинга просматривают события сетевого трафика. IDEF-диаграмма бизнес-процесса мониторинга, приведена на рис. 3 [3]. При этом, анализу подвергаются как поток данных через сеть, так и сами данные. Агенты инвентаризации регистрируют параметры программных и аппаратных средств ИС. Агенты системного мониторинга фиксируют события в операционной системы (ОС). Агенты все результаты мониторинга записывают базу данных.

Множество средств аудита:

$$CA = \{ a_l \}, \quad (5)$$

где $a_l$ – $l$-ое $CA$, $l=1,\ldots L,L$ – количество средств аудита (агентов) в СЗИ;

$$a_l=\{ A_{l1}, A_{l2}, \ldots, A_{ln} \}, \quad (6)$$

$A_{ln}$ – $n$-й параметр, проверяемый $l$-м агентом аудита на соответствия требованиям, при условии, что $a_l \in m_k$.

Агенты аудита устанавливают и причинно-следственную связь снижения относительного риска и осуществляют выбор управляющих решений из базы данных для устранения этого снижения. Управляющие решения – это список *МЗ,* в которых необходимо установить новые режимы работы (перевести в новые состояния). В тех случаях, когда такую связь не удается установить, то администраторы информационной безопасности, вырабатывают новые управляющие решения, в том числе, и возможно за счет замены *МЗ* на новые или расширения типов *МЗ.* IDEF-диаграмма бизнес–процесса управления информационной безопасностью приведена на рис. 4.

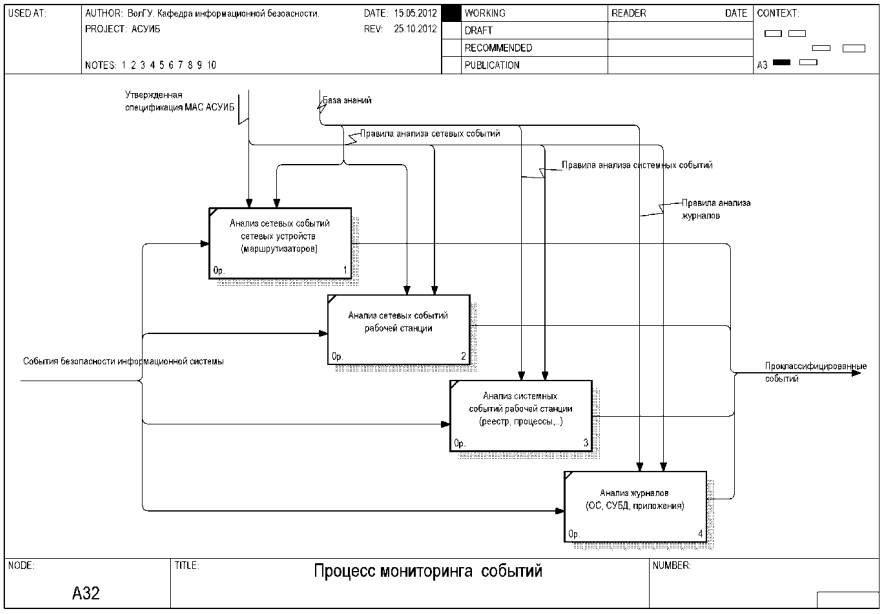


*Рис. 3. IDEF-диаграмма бизнес–процесса мониторинга*

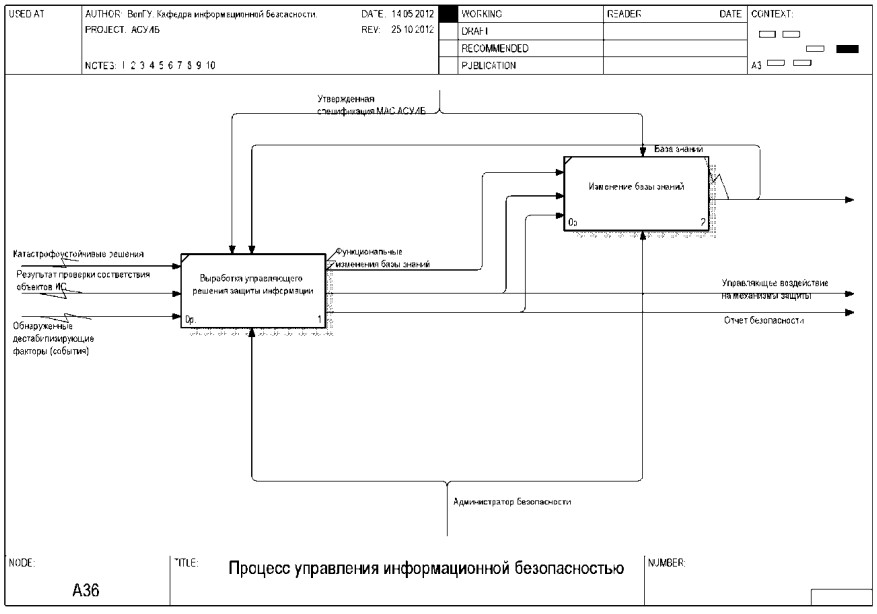


*Рис. 4. IDEF-диаграмма бизнес–процесса управления информационной безопасностью*

**Практическая значимость.** Результаты тестовых проверок работы автоматизированной системы управления информационной безопасностью предприятия.

В ИС предприятия установлено два *МЗ:*$s_1$ – антивирус, $s_2$ – межсетевой экран.

Формальная модель. Для$s_1П_1$= {$П_{11}$, $П_{12}$, $П_{13}$}, где $П_{11}$ = низкий уровень защиты, $П_{12}$=рекомендуемый уровень защиты, $П_{12}$=высокий уровень защиты. На $s_1$установлен режим $П_{11.}$ Для $s_2П_2$={$П_{21}$, $П_{22}$}, $П_{21}$ = включена фильтрация ip пакетов, $П_{22}$ = выключены фильтрация ip пакетов. На $s_1$установлен режим $П_{22}$ по умолчанию.

В процессе эксплуатации средство мониторинга зафиксировало событие 4616 – RPC (удалённый вызов процедур) – это может привести нарушение целостности при расшифровке входящего сообщения. Вероятность реализации атаки близка 1. Относительный ущерб большой. Рассчитанный относительный уровень риска превосходит заданный относительный риск. Требуется смена состояний (режима работы) межсетевого экрана. Причинно-следственная связь возникновение данного события связана с перенаправлением трафика через хост злоумышленника для подмены содержимого пакета. В базе данных имеется типовое решение для исключения повторов такой атаки необходимо «включить и настроить фильтрацию сетевых пакетов».

В процессе эксплуатации средство мониторинга зафиксировало возникновение события 4688 – создания нового процесса. В нем TokenElevationTypeDefault равен 3, т.е. процесс был запущен с правами администратора. Подобного действия не должно возникнуть на АРМ пользователя, вероятней всего для этого использовался вредоносный код. Вероятность реализации атаки близка 1. Относительный ущерб большой. Рассчитанный относительный уровень риска превосходит заданный относительный риск. Причинно-следственная связь возникновение данного события связана с низким уровнем безопасности антивируса. Если бы антивирус был настроен с более высоким уровнем безопасности, то вредоносный код, спровоцировавший запуск процесса был бы обнаружен антивирусным средством. Требуется смена состояний (режима работы) антивирусной программы. В базе данных имеется типовое решение – увеличении уровня защищенности антивирусного средства, для нейтрализации последствия запуска вредоносной программы.

Первые результаты исследований проводимых на модели системы автоматизированного управления ИБ предприятия показывают, возможность автоматизировано обрабатывать и реагировать на события ИБ в ИС, и тем самым управлять информационной безопасностью предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Машкина И.В.* Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: Дисс. … д-ра техн. наук. – Изд. ГОУ ВПО Уфимский государственный авиационный технический университет, 2009. – 332 с.
2. *Емельянов В.В., Ясиновский С.И.* Имитационное моделирование систем: Учеб. пособие. – М.: Изд-во МГТУ им. Баумана, 2009. – 584 с.
3. *Цыбулин А.М., Никишова А.В. Умницын М.Ю.* Исследование противоборства службы безопасности и злоумышленников на многоагентной модели // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 94-99.
4. Методология функционального моделирования IDEF0: Руководящий документ / ИПК Издательство стандартов, 2000.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

**Цыбулин Анатолий Михайлович** – Волгоградский государственный университет; e-mail: anatsybulin@yandex.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; зав. кафедрой.

**Tsybulin Anatoly Mihaylovich** – Volgograd State University; e-mail: anatsybulin@yandex.ru; 100, pr. Universitetsky, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; head of department.