

МОДЕЛЬ ИНТЕГРИРОВАННОЙ СИСТЕМЫ МЕНЕДЖМЕНТА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЛОЖНЫХ ОБЪЕКТОВ

Лившиц И.И.¹, Фаткиева Р.Р.²

Для создания современных систем управления важно обеспечить заданные режимы функционирования и параметры контроля объекта. Проблема принятия решения подразумевает решение ряда задач, в частности, оценку информации о проблемной ситуации в интегрированной системе менеджмента. Предложено формировать модель проблемной ситуации на базе именно интегрированных систем, принимая во внимание современные требования к информационной безопасности. Однако в настоящее время не создано единого подхода к формированию интегрированных систем, что не позволяет в должной мере реализовать безопасное управление сложными промышленными объектами посредством периодической оценки результативности аудитов информационной безопасности. В данном исследовании предпринята попытка анализа систем управления для сложных промышленных объектов с позиции формирования модели проблемной ситуации.

Ключевые слова: Система управления, интегрированная система менеджмента; информационная система; информационная безопасность; аудит.

DOI: 10.21681/2311-3456-2018-1-64-71

Список сокращений:

ИБ – информационная безопасность;
ИТ – информационная технология;
КС – кибернетическая система;
ЛПР – лицо, принимающее решение;

СлПО – сложный промышленный объект;
СУ – система управления;
ТС – техническая система;
ФБ – функциональная безопасность.

Введение

При создании современных систем управления (СУ) представляется важным обеспечение не только заданных технологических режимов сложных промышленных объектов (СлПО), но и достижение определенной цели — безопасного функционирования информационных систем (ИС) в составе конкретных СлПО. Применительно к специфике функционирования СлПО, особое актуальное значение приобретает обеспечение информационной безопасности (ИБ). Расширение термина ИБ (не только «классическая триада»: конфиденциальность, целостность и доступность (см. ISO/IEC 27001), нашло свое практическое применение и в иных документах (IEC 61508, IEC 61511). Обеспечение ИБ (security) предлагается трактовать как компонент более общей задачи – обеспечение функциональной безопасности (ФБ, safety) для СлПО (IEC 61508, п. 3.1.11).

Обзор существующих методик

При изучении проблемы принятия решения при формировании СУ для СлПО применяются различные методики, в том числе: исследование модели проблемной ситуации и учет различных

компонент (внутренних и внешних подсистем). Эти методики описаны в работах [1 – 5] и ряда зарубежных ученых [6, 7]. В работе [1] отмечается «хаотическая динамика» и междисциплинарная природа сложных технических систем (ТС). Общий анализ условий безопасного функционирования СлПО представлен в работе [2]. В работе [3] отмечается, что «мониторинг, прогнозирование и управление СлО на практике автоматизировано лишь частично». В работе [8] представлен тезис, что «в процессе объединения отдельных наук актуальны вопросы создания критериев комплексной оценки при проявлении кризисов различного рода (катаклизмов)», и есть основание выбрать одну из основных целей создания современных СУ как раз противодействие таким «кризисам».

Применимые требования

В данной работе применяется расширенный «классический» термин ИБ для свойств обеспечения безопасного функционирования СлПО. Для решения проблемы обеспечения ИБ в СУ для СлПО, как проблемы выбора лиц, принимающих решения (ЛПР), необходимо представить ее в виде

1 Лившиц Илья Иосифович, кандидат технических наук, Университет ИТМО, г. Санкт-Петербург, livshitz.il@yandex.ru

2 Фаткиева Роза Равильевна, кандидат технических наук, доцент, СПИИРАН, г. Санкт-Петербург, rff@ias.spb.su

ряда задач и сформировать модель проблемной ситуации (в нотации, представленной в [15]). В IEC 61508 отмечается: «компьютерные системы..., во все более увеличивающихся объемах используются для выполнения функций обеспечения безопасности» (IEC 61508 п. 1.2, а) и/или «требует рассмотрения злонамеренных и непредусмотренных действий во время анализа отказов и рисков» (IEC 61508 п. 1.2 к). В стандарте IEC 61511 отмечено, что «в большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. При необходимости он может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск» (IEC 61511, п. 1.2. е).

Под открытой системой понимается СУ СлПО, в состав которой входят ИС, для которых необходимо обеспечение ИБ, в том числе, обеспечение ФБ (в терминах 8, 9]). В справочнике по эффективности ТС показано, что ТС со слабо предсказуемым поведением относят к сложным, и именно данный тип ТС обладает важным признаком – способностью принимать решения, что особо актуально для области ИТ. Также отмечается, что для достижения поставленной цели следует применять классическое значение операции, точнее, вовлечение средств (систем), непосредственно взаимодействующих с «активными средствами». К таким «активным средствам» операции относят как ТС, так и ресурсы, в том числе и информационные. Эти средства могут объединяться в подсистемы, образуя новые управляющие контура обратной связи, в частности – аудит ИБ. В эту гипотезу хорошо укладывается и предложение включать в состав таких управляющих подсистем «распорядительные центры» (в нотации [15, стр. 12]).

Постановка задачи

Для выбора объектов, подлежащих дальнейшему рассмотрению, из множества имеющихся, ЛПР руководствуется своей системой предпочтений, которая базируется на измерениях (формальных контрольных процедурах). Обозначим (в нотации [15]):

U – множество стратегий ЛПР;

A – множество значений определенных и неопределенных факторов;

G – множество исходов операции;

Y – вектор характеристик исхода $g \in G$ (числовое выражение результаты операции);

W – показатель эффективности;

Ψ – оператор соответствия «результат – показатель»;

K – критерий эффективности;

H – модель соответствия множеств: $H: U \times A \rightarrow Y (G)$

Ω – модель предпочтений ЛПР на элементах множества: $D = \{U, A, G, Y, W, K\}$,

θ – общая информация о проблемной ситуации.

Тогда модель проблемной ситуации описывается в нотации [15] как:

$$\langle U, A, H, G, Y, \Psi, W, K, \Omega, \theta \rangle \quad (1)$$

Для решения проблемы принятия решения ЛПР требуется определить состав общей информации о проблемной ситуации (θ), как важнейший элемент формирования оперативных и эффективных управленческих решений, основанных на объективных достоверных данных. В качестве ограничений рассматриваются сроки ожидания ЛПР, допустимые затраты.

Оценка общей информации о проблемной ситуации

Современный этап развития теории управления и, соответственно, синтез СУ, включает в себя не только моделирование физических аспектов функционирования систем обеспечения ИБ (насколько это необходимо для создания адекватной модели), но и учет экономических факторов. Вторая (экономическая) часть СУ необходима для учета внешних аспектов любой открытой системы («issues» - в терминах ISO/IEC 27001, ISO 19011) и разнородной структуры требований. Влияние указанных аспектов позволяет осуществить учет разнородной структуры требований безопасности, на базе которых формируется новая информация о проблемной ситуации θ_N . Обладая актуальной θ_N , ЛПР последовательно формирует компоненты (1), в частности: подмножества $U_N (U_N \in U)$ и $A_N (A_N \in A)$. Аналогично выбираются характеристики Y_N для исходов G_N и устанавливается H_N как $H_N: U_N \times A_N \rightarrow Y_N (G_N)$. Далее с учетом Y_N формируется Ψ_N как $\Psi_N: \{ U_N \times A_N \rightarrow Y_N (G_N) \} \rightarrow W_N$.

Отметим, что в работе [4] дано уточнение: «под средой понимается не физическое окружение объектов, а абстрактная модель совокупности факторов, о которых у нас нет достоверной информации» и далее: «если неопределенные факторы удаётся описать в виде случайных величин... с известной функцией распределения, то говорят, что возмущающие действия статистически распределены». На основании этого базового требования представляется возможным формировать объективную информацию о проблемной ситуации.

Формирование общей модели объекта

Построение обобщенной модели СУ начинается с построения модели объекта управления (в данном конкретном случае объектом управления является СлПО) и затем – формирования начальных условий, которые определяют состояния объекта управления в дискретные моменты времени (t_1, \dots, t_k). Различные состояния возможно отследить, начиная от начального состояния СУ для СлПО — Z_1 , и далее под воздействием условий к состоянию ΔZ_1 . Состояния СУ предлагается обозначать как Z_1, Z_2, \dots, Z_k . В рассматриваемой системе каждый компонент под воздействием особых условий («условия принуждения» в терминах [8]) меняет свое состояние: $Z_1 \rightarrow Z_2$. Соответственно, это позволяет предложить общую схему формирования пространства состояний Z_k (рис. 1).

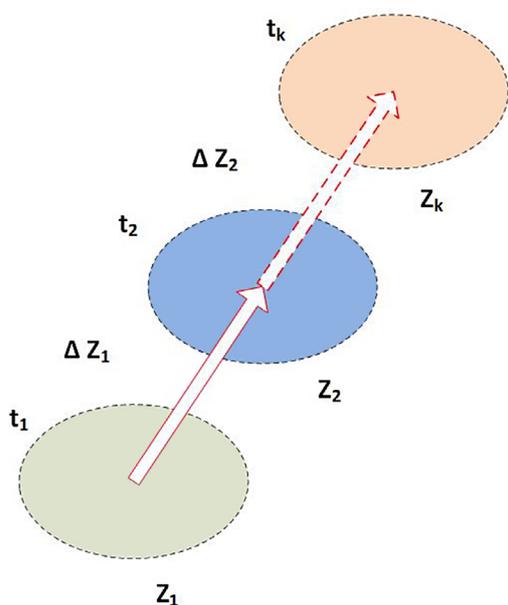


Рис. 1. Формирование пространства состояний открытой системы

В этой схеме учтены начальное состояние Z_1 , воздействия («условия принуждения») перехода в последующие состояния (ΔZ_1) и дискретные моменты времени (t_1, \dots, t_k), в которые должна анализироваться новая информация об изменении проблемной ситуации. В работе [15] показано, что модель должна адекватно отображать исследуемые операции с т.з. информационных связей, и рекомендуется рассматривать модель как «кибернетическую систему» (КС). В смысле моделирования КС для целей обеспечения ИБ принципиально важно, что в данном конкретном случае рассматриваются именно «поведенчески неоднозначные систем» («нерефлексные» в нотации [15]).

Рассмотрим далее пример СлПО и представим более подробное описание параметров модели с учетом обеспечения ФБ.

Общая модель объекта

Рассмотрим общую модель более сложной системы, которая включает СлПО (как объект управления) и СУ, реализованную на базе ИСМ для СлПО (рис. 2). Для обеспечения ИБ СлПО важно определить размерность пространства состояний модели ИСМ для корректного описания аспектов моделирования СлПО. Предлагается ввести в практику оценки новые параметры на основе указанных выше принципов (например, ИЕС 615011):

- границы оценки ФБ;
- ресурсы, необходимые для оценки безопасности;
- уровень его сложности;
- уровень полноты безопасности;
- последствия в случае отказа;
- уровень стандартизации проектных решений;
- нормативные требования безопасности.

Отдельно следует принять во внимание «специализацию» СлПО по отраслям и наличие особых требований ИЕС 61511, например, «мешающий» (ложный) отказ (п. 3.2.65), участие человека как части системы (п. 3.2.92). Дополнительно отметим непосредственное влияние отраслевых аспектов ФБ на частную задачу, например, защиту ключей или паролей (п. 11.7.1.3), защиту конфигурации логических устройств и обеспечение целостности (п. 11.5.5.5). Некоторые аспекты оценки результативности программ аудитов ИБ для конкретного СлПО описаны в работах [10 – 12]. Предложенная общая модель ИСМ для обеспечения безопасности СлПО (рис. 2) может выступать в качестве новой основной модели, обеспечивая поиск конкретных альтернатив за счет гибких обратных связей (аудитов ИБ). Процесс аудита может предоставлять численные оценки и поддерживать эффективное решение задачи обеспечения безопасности СлПО. В дополнение к определению роли нового блока аудита в составе ИСМ и оценки его воздействия на СлПО (как объект управления) отметим, помимо «классических» требований ИБ, также и требования ФБ (ИЕС 61508), в частности:

- определение требований к периодическому аудиту ФБ, включая частоту проведения аудита, уровень независимости стороны и программу выполнения аудита (п. 6.2.7);
- анализ опасностей и рисков, формирование области распространения (п. 7.1.2.2);
- определение опасных событий и ситуаций (включая условия возникновения отказов, разумно

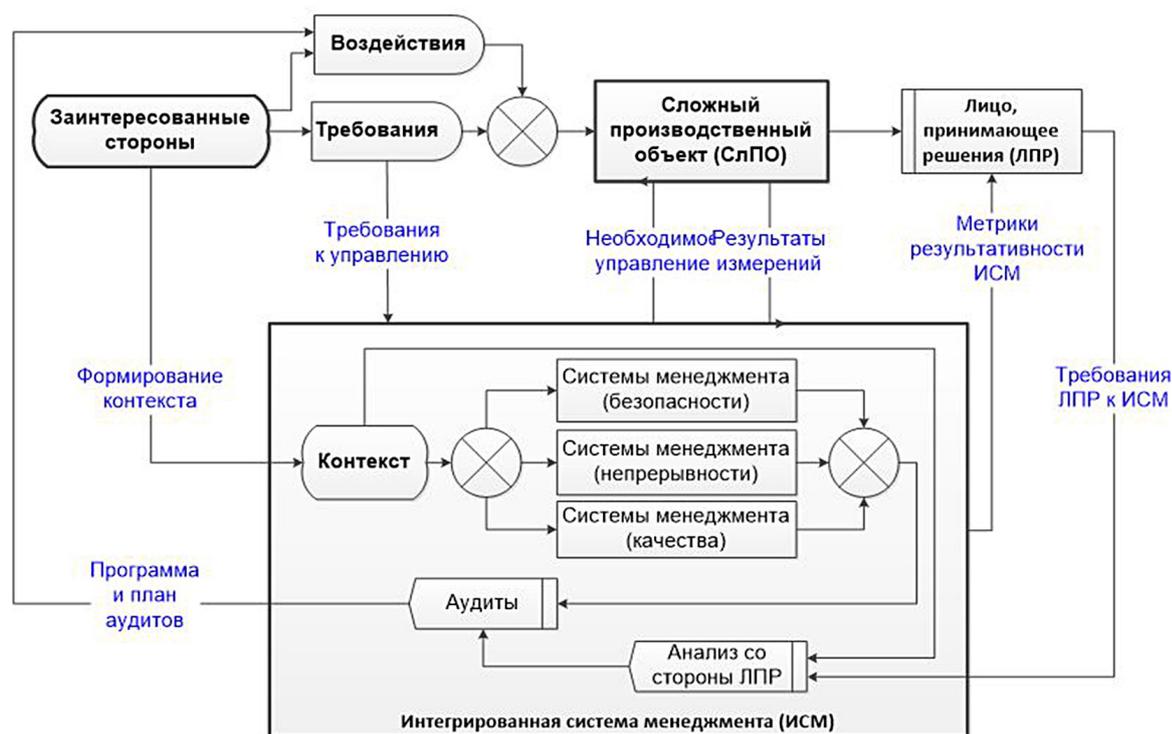


Рис. 2. Общая модель ИСМ для обеспечения безопасности СлПО

предсказуемое неправильное использование или несанкционированные действия), включая случаи, связанные с человеческим фактором (п. 7.4.2.3).

С учетом применения риск-ориентированных стандартов в ИСМ важным представляется гарантирование «замыкания» цикла PDCA при управлении ИБ СлПО и формирование контекста для управления СлПО как «открытой системы» в терминах И. Пригожина [14].

Эффективность операций в СлПО

Операция, как процесс функционирования «S₀-системы» (в нотации [15]), описывается набором определенных параметров. Отметим, что в состав «S₀-системы» входят и ТС и «распорядители». Совокупность конкретных значений этих параметров в фиксированный момент времени, называется «состоянием системы» (рис. 1). Функционирование системы заключается в последовательной смене состояний системы, и этот процесс должен находиться под контролем «распорядительного центра» в общем и конкретно – ЛПР. [15, стр. 13]. В каждый момент времени система может находиться только в одном определенном состоянии, и это состояние называется «ситуацией» (в нотации [15]). Это хорошо коррелирует с практикой аудитов СлПО, при которой оценивается не ежегодное статическое положение системы, а постоянные системные улучшения [12]. Следующий вопрос касается

формирования непосредственно оценки эффективности операции (в предложенной идее – как процесса аудита ИБ для СлПО) через оценивание совокупности факторов, существенно влияющих на изменение обстановки («условия обстановки» в нотации [15, стр. 13]). К таким факторам предлагается отнести, например, следствия активного противодействия (в нотации ISO/IEC 27001), а именно – возможности, характер, способы противодействия и виды атакуемых ресурсов (технические, финансовые, временные и пр.). Эти факторы образуют уточненное пространство временных, технических, ресурсных, технологических и иных ограничений, которые должны быть учтены при решении поставленной задачи.

Факторы в нотации ISO/IEC 27001, в отличие от действующих методических документов регуляторов в РФ, разделяются на управляемые (контролируемые) и неуправляемые. Для ЛПР именно управляемые факторы являются целями (подцелями) при планировании, проведении и анализе результатов аудита ИБ, поскольку показывают степень «успешности» оперативного управления конкретной ТС [15, стр. 20]. Если некоторая ТС для каждой цели показывает достаточную эффективность, можно говорить о наличии широких функциональных возможностей. Применительно к цели аудита ИСМ для СлПО можно привести аналогичный пример, по которому оценка

эффективности каждой СМ демонстрирует высокую эффективность ИСМ, и в том числе – в аспекте обеспечения ИБ [13].

Для исследования эффективности операций ТС приемлемо рассматривать «потенциальную эффективность», как основную характеристику качества конкретной ТС. Для новой предложенной оценки предлагается применять аппарат аудитов ИБ, который позволяет предоставлять численные метрики конкретного СлПО («системной оболочки») и, в частности, оценки степени обеспечения ИБ для СМИБ (как отдельной системы) или ИСМ (как подсистемы). Именно для СлПО удобно расширить термин «качество ТС» (в нотации [15]) на устойчивость, управляемость и пр., что хорошо коррелирует с требованиями стандартов в области ФБ. Отметим также новый стандарт ISO 22316 версии 2017 «Security and Resilience - Organizational Resilience - Principles and Attributes», который затрагивает вопрос «киберустойчивости».

В общей практике аудитов ИБ удобно расширить оценку результативности (как степени достижения цели) на гомеостазис, как способность ТС возвращаться в равновесное состояние после возмущающих воздействий [15, стр. 18]. Отмечается, что в «гомеостатических» системах (в нотации [15] – «*h-системах*») управление сводится к функции регулирования, что отлично согласуется с общей практикой аудитов ИБ в ИСМ для СлПО. Для цели аудитов ИБ в ИСМ для СлПО крайне важно фиксировать устойчивое состояние в конечное время, заданное, например, в виде программы аудитов ИБ. Важно также не допустить «срыв» управления, иначе говоря, ЛПР необходимо контролировать «замыкание» каждого цикла PDCA для всех подсистем в ИСМ. Отметим, что требование «замыкания» цикла PDCA важно именно в аспекте исполнения аудитов ИБ как оценивание «качества» СУ, в частности – периодическое измерение «рассогласования» между заданными ЛПР целевыми показателями и текущим результатами аудитов.

Рассмотрим виды факторов, которые ЛПР следует принять во внимание при планировании аудитов ИБ в ИСМ: определенные (которые известные с требуемой точностью) и неопределенные (случайные). Наибольшей неопределенностью обладают факторы с неизвестной функцией принадлежности, т.е. диапазонами изменения переменных. К ним применяют процедуры только экспертного оценивания диапазонов изменений их значений [15, стр. 22]. Определим показатель эффективности (в нотации [15]) как $W(u)$, т.е. меру степени соответствия результата операции (по

факту) требуемому ЛПР (план). Примем во внимание также новое дополнительное понятие «результативность», как степень соответствия цели СУ для СлПО. Также дополнительно примем во внимание 3 концепции рационального поведения ТС для выработки решений (в нотации [15]): пригодности, оптимизации и адаптивизации. Для целей конкретного применения модели аудитов ИБ в ИСМ для СлПО более подробно рассмотрим именно адаптивизацию. Это решение объективно обосновывается фактом, что именно для целей аудита ИБ указанная выше концепция предполагает возможность оперативного реагирования в ходе операции на поступающую текущую информацию об изменении возмущающих воздействий [13]. Тогда с учетом модели проблемной ситуации (1) формирования новой информации θ_N определим новый показатель эффективности:

$$W(u) = \rho(Y(u) + Y^{TP} + Y^R + Y^{RR}) \quad (2)$$

где:

- $Y(u)$ – результат операции при некоторой стратегии,
- Y^R – результат противодействия ожидаемому выполнению операции при некоторой стратегии ($Y_R \neq 0$),
- Y^{RR} – результат адаптивизации ТС при конкретном применении операции при известном противодействии Y^R при некоторой стратегии,
- Y^{TP} – требуемый результат операции при условии, что $Y(u)$, Y^R , Y^{RR} и Y^{TP} неслучайные величины.

Отметим, что допускается введение в выражение (2) дополнительной оценочной функции, показывающей склонность ЛПР к риску и формирования специальной «субъективной» (в нотации [15]) оценочной функции. В дальнейшем будем применять только «объективные» показатели эффективности операций. Рассмотрим критерий эффективности K , который вводится на основе предположения рационального поведения ЛПР (что хорошо коррелирует с «разумным поведением» ЛПР в нотации Р. Кини и Х. Райфа) и позволяет сопоставить различные стратегии достижения цели. Соответственно, в данном конкретном случае для СлПО должна применяться новая концепция адаптивизации, заключающаяся в изменении стратегии управления на основе информации, получаемой посредством подсистемы аудитов ИБ (рис. 2). Более того, накапливая такую объективную информацию (Y^R и Y^{RR}), ЛПР может оперативно строить «прогнозные» стратегии и, при необходимости, обоснованно менять цели.

Таким образом:

$$W_t(u^*(t), \tau) \geq W_t^{TP}(u^*(t), \tau); u(t) \in U(t, \tau)$$

где:

t – время;

τ – прогнозное упреждение.

Запись W_t означает динамическую природу изменения показателя эффективности, что может быть увязано с ранее предложенной концепцией «мгновенных аудитов» [13].

Новая модель проблемной ситуации

В соответствии с нотацией [15] определим новую модель проблемной ситуации. На основании имеющейся информации θ_N и результатов «контрольного» оценивания (аудита) ИБ СлПО необходимо определить модель предпочтений ЛПР – Ω [15, стр. 59], приведенную в (1). Отметим, что наличие A в (1) означает, что часть значений неопределенных факторов будет установлена (например, правила проведения аудитов ИБ заданы регуляторами), либо будет решаться как самостоятельная задача (например, перечень средств обеспечения ИБ, рекомендованных ЛПР к внедрению). Как показано в работе [15], во многих практических случаях априорное значение коэффициента эффективности K приводит к формированию множества «нехудших альтернатив». Это означает, что по результатам аудитов ИБ могут быть сформированы несколько альтернатив, а мера выбора определяется ЛПР посредством модели предпочтения Ω . Общая постановка за-

дачи моделирования предпочтений может быть представлена в виде:

$$\langle D, \theta_N; \Omega_D \rangle \quad (3)$$

где:

$$D = \{U, A, G, Y, W, K\}$$

θ_N – иная информация о проблемной ситуации.

Предлагается расширить состав информации о проблемной ситуации θ_N за счет новых факторов и представить задачу формирования множества стратегий ЛПР в новом виде:

$$\langle \theta_{A0}, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, A_N, U_N \rangle \quad (4)$$

где:

- θ_{A0} – информация о начальной (исходной) цели операции;
- θ_1 – информация о результативности «мгновенных аудитов» ИБ;
- θ_2 – информация о результативности аудитов всех типов (первой, второй и третьей стороной);
- θ_3 – информация об инцидентах ИБ (например, от Security Operation Center (SOC) и пр.);
- θ_4 – информация о новом «контексте» СМИБ (ИСМ);
- θ_5 – информация о новых предпочтениях ЛПР;
- θ_6 – информация о важных изменениях (например, ФЗ-187 «ГоСОПКА»).

Отметим, что переход от общей модели к модели «конкретной ситуации» является очень сложным, особенно когда речь идет об анализе ТС (в том числе – СлПО) [15, стр. 74]. В ряде случаев

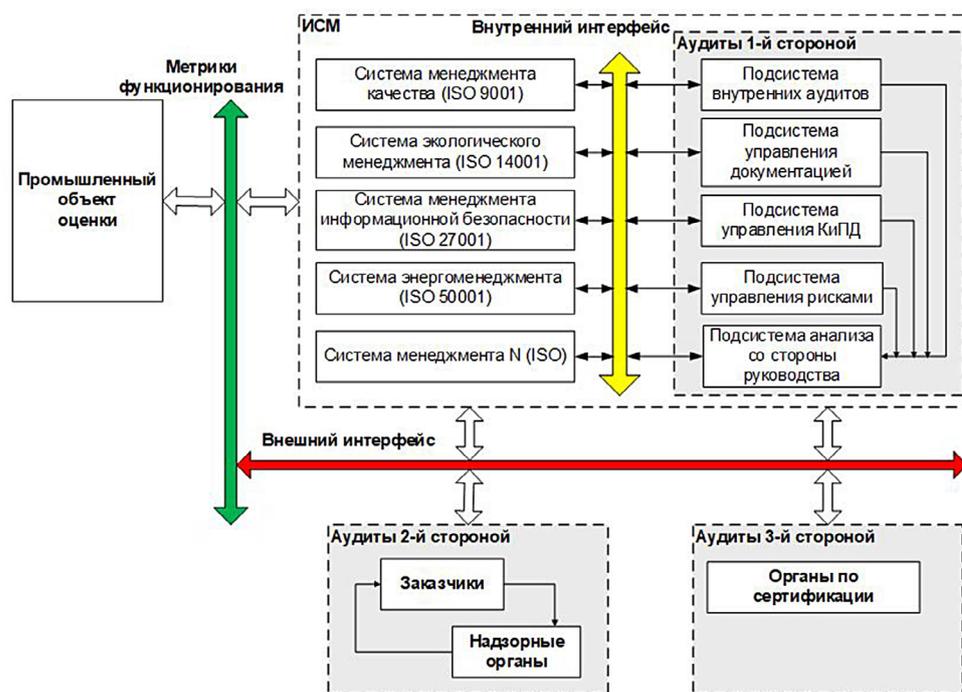


Рис. 3. Базовая модель аудитов ИСМ

применяются только эвристики, т.к. многие компоненты явно не заданы [15, стр. 55]. Кроме того, новацией в развитии модели аудитов ИБ является постоянная оценка адекватности, конкретные механизмы которой (например, циклы оптимизации) рассмотрены ранее в [13]. Принимая во внимание общую модель ИСМ (рис. 2) и основные ограничения, которые должны быть учтены, предлагается базовая модель аудитов ИСМ (рис. 3).

В этой модели, как части общей модели ИСМ (рис. 2), детально отражена возможность сопоставлять планируемые и реальные состояния СУ для СлПО (как объекта оценки – ОО), реализуется «замкнутый» цикл аудитов (выполнение всех обязательных процедур аудита ИБ согласно ISO 19011). Для конкретной задачи управления ИБ в СУ для СлПО «замкнутый» цикл аудитов означает гарантированное достижение результатов всех фаз PDCA, выявления несоответствий и результативное выполнение корректирующих действий [13]. В базовой модели аудитов ИСМ вводятся различные интерфейсы предоставления данных (внутренний и внешний), что отражает требования

стандартов ИБ, учитывает требования ЛПП в части ограниченного распространения чувствительных данных [11] и учитывает необходимость коммуникаций открытой системы с внешней средой с позиции энергетического обмена [14].

Выводы

Для оценивания информации о проблемной ситуации, необходимой для формирования управляющих решений, могут быть применены новые критерии. Предложена модель ИСМ для обеспечения безопасности СлПО, которая учитывает новые параметры выполнения аудитов ИБ. Предложено при обеспечении безопасности СлПО дополнительно учитывать концепцию рационального поведения и, прежде всего, «адаптивизацию», что дополнительно учитывает оперативное реагирование на поступающую информацию об изменении возмущающих воздействий. В новой модели проблемной ситуации для СлПО учитывается расширенная информация о проблемной ситуации, в том числе – результативность аудитов ИБ, что позволяет сократить для ЛПП выбор из «нехудших» альтернатив.

Рецензент: Молдовян Александр Андреевич, доктор технических наук, профессор, начальник научно-исследовательского отдела проблем информационной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН), г. Санкт-Петербург, тел. (812)328-51-85; E-mail: maa1305@yandex.ru.

Литература

1. Агуреев И.Е., Тропина В.М. Динамика логистической системы в транспортных цепях поставок // Известия Тульского государственного университета. Технические науки. 2011. № 4. С. 158-167.
2. Агуреев И.Е., Богма А.Е., Пышный В.А. Динамическая модель транспортной макросистемы // Известия Тульского государственного университета. Технические науки. 2013. № 6-2. С. 139-145.
3. Охтилев М.Ю., Соколов Б.В. Новые информационные технологии мониторинга и управления состояниями сложных технических объектов в реальном масштабе времени // Труды СПИИРАН. 2005. Т. 2. № 2. С. 249-265.
4. Соколов Б.В., Потрясаев С.А., Малышева И.В., Назаров Д.И. Алгоритм адаптации моделей управления структурной динамикой сложной технической системы к воздействию возмущающих факторов // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 3-6.
5. Алабян А.М., Зеленцов В.А., Крыленко И.Н., Потрясаев С.А., Соколов Б.В., Юсупов Р.М. Оперативное прогнозирование наводнений на основе комплексного упреждающего моделирования и интеграции разнородных данных // Труды СПИИРАН. 2015. № 4. С. 5-33.
6. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds // J. Mechanics of Structures and Machines. 1995. Vol. 23. P. 135-158.
7. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer, 2005. 684 p.
8. Игонин В.И. Технологические особенности энергообследования зданий, сооружений и инженерных сетей. Курс лекций. Вологда: ВоГТУ. 2012. 104 с.
9. Аюров В.Д. Круговорот товаров и физика денег // Горный информационно-аналитический бюллетень. 2003. № 5. С. 90-91.
10. Лившиц И.И. Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. № 1. С. 22-34.
11. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. № 6. С. 72-94.
12. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. № 3. С. 10-15.
13. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. 2015. № 6. С. 253-270.
14. Пригожин И., Гленсдорф П. Термодинамическая теория структуры, устойчивости и флуктуаций. М.: МИР. 1973. 124 с.
15. Надежность и эффективность в технике: Справочник в 10 т./ Ред. совет: В.С. Авдучевский, (пред.) и др. – М.: Машиностроение, 1988. – (в пер.) Т. 3. Эффективность технических систем/Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. – 328 ст.: ил.

THE INTEGRITY MANAGEMENT SYSTEM FOR SECURITY ENSURING FOR COMPLEX FACILITIES

Livshitz Ilya³, Rosa Fatkueva⁴

Creation the modern management systems is important to ensure the specified modes of operation and parameters of control object. The problem decision involves the number of tasks, assessing information about a problem situation. The proposed model a problem situation estimate based on integrated management system and taking into account modern IT–security requirements. However, currently there is no common approach to the formation of integrated systems, which does not allow to adequately implementing controls of complex industrial facilities through periodic evaluation of the effectiveness of IT–security audits. In this issue shows an attempt to analysis of management systems for complex industrial objects from the perspective of forming a model of the problem situation.

Keywords: Management system, Integrated Management System; Information System; Information Security; Audit.

References

1. Agureev I.E., Tropina V.M. Dinamika logisticheskoy sistemy v transportnykh tsepyakh postavok. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2011. No 4, pp. 158-167.
2. Agureev I.E., Bogma A.E., Pyshnyy V.A. Dinamicheskaya model' transportnoy makrosistemy, Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2013. No 6-2, pp. 139-145.
3. Okhtilev M.Yu., Sokolov B.V. Novye informatsionnye tekhnologii monitoringa i upravleniya sostoyaniyami slozhnykh tekhnicheskikh ob'ektov v real'nom masshtabe vremeni, Trudy SPIIRAN. 2005. T. 2. No 2, pp. 249-265.
4. Sokolov B.V., Potryasaev S.A., Malysheva I.V., Nazarov D.I. Algoritm adaptatsii modeley upravleniya strukturnoy dinamiko slozhnoy tekhnicheskoy sistemy k vozdeystviyu vozmushchayushchikh faktorov, Vserossiyskaya nauchnaya konferentsiya po problemam upravleniya v tekhnicheskikh sistemakh. 2015. No 1, pp. 3-6.
5. Alabyan A.M., Zelentsov V.A., Krylenko I.N., Potryasaev S.A., Sokolov B.V., Yusupov R.M. Operativnoe prognozirovaniye navodneniy na osnove kompleksnogo uprezhdayushchego modelirovaniya i integratsii raznorodnykh dannykh, Trudy SPIIRAN. 2015. No 4, pp. 5-33.
6. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds, J. Mechanics of Structures and Machines. 1995. Vol. 23, pp. 135-158.
7. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer, 2005. 684 p.
8. Igonin V.I. Tekhnologicheskie osobennosti energoobsledovaniya zdaniy, sooruzheniy i inzhenernykh setey, Kurs lektsiy. Vologda: VoGTU. 2012. 104 P.
9. Ayurov V.D. Krugovorot tovarov i fizika deneg, Gornyy informatsionno-analiticheskiy byulleten'. 2003. No 5, pp. 90-91.
10. Livshits I.I. Prakticheskie primenimye metody otsenki sistem menedzhmenta informatsionnoy bezopasnosti, Menedzhment kachestva. 2013. No 1, pp. 22-34.
11. Livshits I.I. Podkhody k primeneniyu modeli integrirovannoy sistemy menedzhmenta dlya provedeniya auditov slozhnykh promyshlennykh ob'ektov – aeroportovykh kompleksov, Trudy SPIIRAN. 2014. No 6, pp. 72-94.
12. Livshits I.I. Metodika vypolneniya kompleksnykh auditov promyshlennykh ob'ektov dlya obespecheniya effektivnogo vnedreniya sistem energomenedzhmenta, Energobezopasnost' i energosberezhenie. 2015. No 3, pp. 10-15.
13. Livshits I.I. Formirovaniye kontseptsii mgnovennykh auditov informatsionnoy bezopasnosti, Trudy SPIIRAN. 2015. No 6, pp. 253-270.
14. Prigozhin I., Glensdorf P. Termodinamicheskaya teoriya struktury, ustoychivosti i fluktuatsiy. M.: MIR. 1973. 124 P.
15. Nadezhnost' i effektivnost' v tekhnike: Spravochnik v 10 t. / Red. sovet: V.S. Avduevskiy, (pred.) i dr. – M.: Mashinostroenie, 1988. – (v per.) T. 3. Effektivnost' tekhnicheskikh sistem/Pod obshch. red. V.F. Utkina, Yu.V. Kryuchkova. – 328 P.: il.



³ Livshitz Ilya, Ph.D., ITMO University, Saint-Petersburg, livshitz.il@yandex.ru

⁴ Fatkueva Roza, Ph.D., SPIIRAS, Saint-Petersburg, rrf@iiias.spb.su