УДК 004.94 **DOI** 10.15622/sp.48.3

И.И. Лившиц

МЕТОДИКА ОПТИМИЗАЦИИ ПРОГРАММ АУДИТА ИНТЕГРИРОВАННЫХ СИСТЕМ МЕНЕДЖМЕНТА

Лившиц И.И. **Методика оптимизации программы аудита интегрированных систем менеджмента.**

Аннотация. Применение интегрированных систем менеджмента (ИСМ) в настоящее время привлекает внимание высшего руководства самых разных организаций: нефтеперерабатывающих, приборостроительных, авиационных и оборонных. Однако, на данный момент остается важной проблемой выполнение аудита в ИСМ — реализация в полном объеме комплекса проверок различных стандартов ISO при ограничении или существенном сокращении доступных ресурсов.

В то же время постоянное совершенствование принципов управления, и в частности переход к мышлению, основанному на рисках, обеспечивают повышение интереса к рациональному применению стандартов ISO. В данном исследовании предлагается методика оптимизации программы аудита ИСМ, основанная на принципах непрерывной адаптации при поступлении данных в течение одного микроцикла аудита. Дополнительным преимуществом данной методики является применение численных метрик аудита информационной безопасности, способствующих постоянному повышению уровня обеспечения информационной безопасности организаций.

Ключевые слова: информационная безопасность, интегрированная система менеджмента, стандарт, аудит, система менеджмента информационной безопасности.

1. Введение. В последнее время применение интегрированных систем менеджмента (ИСМ) привлекает внимание высшего руководства (лиц, принимающих решения — ЛПР) различных организаций. Наблюдаются практически единичные случаи, когда современные организации самой разной отраслевой принадлежности (нефтеперерабатывающие, приборостроительные, авиационные и оборонные) внедряют только одну систему менеджмента (СМ), напротив, сейчас, как правило, реализуются именно проекты ИСМ. Рассмотрим несколько крупнейших российских организаций, в которых автору в течение длительного периода 2010–2015 гг. доводилось выполнять аудит ИСМ:

- «КАМАЗ-Дизель» (машиностроение);
- «Теплоком» (приборостроение);
- «Водоканал Санкт-Петербург» (коммунальные услуги);
- «Газпром трансгаз Москва» (транспортировка газа).

В таблице 1 представлены примеры реализации систем менеджмента информационной безопасности (СМИБ).

Однако на данный момент остается важной проблемой обеспечение выполнения программы аудита в ИСМ — реализация в полном объеме комплекса проверок по различным стандартам ISO при

существенном сокращении доступных ресурсов. В большей степени эта проблема характерна для обеспечения программы аудита ИСМ для проверок информационной безопасности (ИБ), поскольку негативные последствия инцидентов ИБ могут привести к существенному ущербу для организации, вплоть до прекращения деятельности.

Таблица 1. Примеры реализации проектов ИСМ

Организация	Стандарты ISO	Национальные стандарты (ГОСТ)	**Источник**
«КАМАЗ-Дизель» (Набережные Челны)	9001 14001 18001 16949 27001	РВ 0015-002-2012	http://www.kamaz.ru/about/policy/labor-protection/; http://www.kamaz.ru/about/quality/system/
«Теплоком» (Санкт-Петербург)	9001 14001 18001 50001	Нет	http://www.teplocom-holding.ru/about/licenses_and_certificates/ http://www.teplocom-holding.ru/about/our_policy/
«Водоканал Санкт-Петербург» (Санкт-Петербург)	9001 14001 18001 50001 27001	Нет	http://www.vodokanal.spb.ru/o_kompanii/ohrana_okruzhayuwej_sredy/ http://www.regcon.ru/index.php/konsalting/ohsas-18001
«Газпром трансгаз Москва» (Москва)	9001 14001 18001 50001 27001	ГОСТ Р ИСО/МЭК 27001-2006	http://moskva-tr.gazprom.ru/ecology/ http://www.rusregister.ru/press-center/association-news/?ELEMENT_ID=15701

В то же время постоянное совершенствование принципов управления, и в частности, переход к мышлению, основанному на рисках, обеспечивают повышение интереса к рациональному применению современных риск-ориентированных стандартов [1-5]. Соответственно, представляет определенный интерес изучение существующих проблем при выполнении аудита ИСМ, а также поиск способов оптимизации программы аудита ИСМ, основанных на принципах непрерывной адаптации при поступлении данных в течение одного микроцикла PDCA (Plan-Do-Check-Act), т.е. одного элементарного цикла аудита. На основании практики выполнения аудитов ИСМ предлагается новая методика оптимизации программы аудита, которая позволит обеспечить более рациональное принятие решений для ЛПР в современной сложной экономической обстановке [6–8].

2. Общие аспекты управления аудитом. Как отмечалось ранее, для обеспечения стабильного развития современных организаций в условиях наличия рисков различного происхождения, представляется целесообразным применение риск-ориентированных стандартов и внедрение ИСМ [9-11, 12-17]. С точки зрения управления аудитом ИСМ в предлагаемой методике отметим необходимость решения следующих важных практических задач (в скобках указаны пункты стандарта аудита СМ — ИСО 19011 [18]):

1. Задача выделения ресурсов для программы аудита:
   - — разработка программы аудита (5.1);
   - — идентификация и оценка рисков программы аудита (5.3.4);
   - — идентификация ресурсов для программы аудита (5.3.6).
2. Задача учета факторов, влияющих на глубину программы аудита утечки, инциденты, проявление криминальных действий, выявленные ранее несоответствия, а следовательно — определение объема программы аудита (5.3.3).
3. Задача сбора верифицируемой информации (6.4.6).
4. Задача обеспечения специальных знаний и навыков аудиторов (7.2.3.3), либо привлечение технических экспертов по следующим областям:
   - — осуществляемые виды деятельности;
   - — требования заинтересованных сторон;
   - — знание процессов обеспечения ИБ;
   - — знание технических средств и мер обеспечения ИБ.

Дополнительно отметим, что в ИСМ должны быть приняты к сведению и рекомендации PAS-99 [5], что позволяет учесть специфические требования выполнения комбинированных аудитов, учета рисков, гибкого управления объемом программы аудита ИСМ с учетом предшествующих результатов и важности процессов [19-21].

3. Принципы организации гибких аудитов. Предлагаемая методика оптимизации программы аудита ИСМ основана на следующих основных принципах:

1. Вводится понятие интегральной оценки (ИО) ИБ, которая включает определенный групповой показатель оценки всех вынесенных на аудит ИБ процессов — R_{ISMS}. Этот групповой показатель определяется с помощью взвешенной суммы частных показателей, в которой весовые коэффициенты определяют важность процесса R_{PR} в организации ИБ для конкретного объекта оценки (ОО).
2. После проведения начального (первичного) аудита ИБ по каждому проверяемому процессу оценивается его состояние на

предмет соответствия требованиям критериев аудита (стандартам ISO, ГОСТ, СТО Газпром СОИБ и пр.), а также его влияние на ИО уровня ИБ для конкретного ОО.

3. Последующие аудиты ИБ проводятся по предложенной методике, использующей гибкий подход: наиболее детально и тщательно подвергаются проверке те процессы, по которым на предыдущем аудите выявлены существенные несоответствия (например, в нотации ISO 17021 — “major” [22]) и которые имеют наибольший приоритет в ИО для конкретного ОО.

4. Частота и детальность, которая должна быть дифференцирована для различных проверяемых процессов, также увязывается с ИО. Например, определенные группы процессов, которые в ИО имеют приоритетное значение (например, в зависимости от модели актуальных угроз ИБ) подвергаются аудитам более детально и чаще. Процессы, имеющие более низкий приоритет в ИО для конкретного ОО, проверяются реже и менее детально.

5. Глубина проверки и частота аудитов каждый раз для k-ого аудита в микроцикле PDCA определяется в зависимости от приближения функции ИО для конкретного ОО к некоему установленному целевому показателю — Rtar (в пределе, очевидно, равным 1) для комплексной оценки защищенности конкретного ОО.

Дополнительно отметим важность внедрения нового стандарта ISO 55000 [2-4], т.к. многие активы не управляются должным образом (например, в силу применения устаревших внутренних процедур СТО Газпром СОИБ в принципе не оперирует такими активами, как персонал, здания, сооружения). Соответственно, применение требований уже внедренного стандарта (например, ISO 27001) значительно облегчает решение «типовых» задач безопасности, которые решаются параллельно (учет и защита активов, управление рисками, оценка компетенции и пр.), рекомендуется к параллельной проверке в рамках совместных аудитов всех СМ [22-24].

4. Математическая постановка задачи. Для оценки степени соответствия системы обеспечения ИБ при аудите ИСМ предъявляемым требованиям ИБ используются частные и групповые показатели ИБ. Например, для целей проведения аудита ИСМ в аспекте обеспечения ИБ предлагается применять показатель результативности СМИБ R_{ISMS}, вычисляемый в каждом цикле k-го аудита по аддитивной формуле (весовой коэффициент *i*-го процесса обозначим как α_i и показатель результативности *i*-го процесса ИБ обозначим как R_{PRi}:

$$R_{ISMS} = \sum_{i=1}^{n} \alpha_i \cdot R_{\Pr i}, \quad (1)$$

при этом сумма весовых коэффициентов α_i нормируется:

$$\sum_{i=1}^{n} \alpha_i = 1.$$

Показатель результативности конкретного *i*-го процесса ИБ R_{PRi}, в свою очередь, вычисляется также по аддитивной свертке метрик ИБ (*j*-ю метрику ИБ для *i*-го процесса ИБ обозначим как K_{KPIij}, а весовой коэффициент — как β_{ij}). В формуле (2) допускается ситуация, когда количество метрик m не будет одинаковым для разных циклов, соответственно, необходимо говорить об m_i:

$$R_{\Pr_i} = \sum_{j=1}^{m_i} \beta_{ji} \cdot K_{PKIji}, \quad (2)$$

при этом сумма весовых коэффициентов β_{ij} нормируется:

$$\sum_{j=1}^{m_i} \beta_{ij} = 1.$$

Сумма весовых коэффициентов частных показателей ИБ, используемых при вычислении группового показателя ИБ, должна быть равной 1, что обеспечивает нормирование всех показателей в аддитивных формулах (1) и (2). Показатель результативности СМИБ R_{ISMS} должен быть в пределе равен 1.

В процессе аудита ИСМ постоянное измерение «невязки» текущего для k-го аудита R_{ISMS} измеряется как рассогласование с целевым показателем $R_{ISMStar}$, и крайне важно обеспечить его минимум. Следовательно, задача оптимизации может быть отнесена к типу задач статической оптимизации для процессов управления, протекающих в установившемся режиме. Необходимо реализовать оптимизационную модель для процесса аудита ИСМ в условиях детерминированных ограничений и условной оптимизации (минимальной «невязки»):

$$F(y) \to \min, \quad (3)$$

где: $F(y) \in R^m$, $f(y) \in R^1$. $f(y)$ — целевая функция m-мерного векторного аргумента ***y***, такого что: $y = (y_1, y_2, \ldots y_m)$. Область допустимых значений $y \in D \subset R^m$. Таким образом, рассматривается вид задачи условной оптимизации. Установленные ограничения (II-го рода, в виде неравенства):

$$g_i(y) \geq 0; i = \overline{1, N}.$$

Параметры m-мерного векторного аргумента ***y*** могут быть, например, следующими:

- T — период аудитов ИБ;
- S — плановая стоимость аудитов ИБ;
- V — объем аудитов ИБ (количество подразделений);
- F — перечень функциональных вопросов аудитов ИБ;
- O — перечень посещаемых объектов аудитов ИБ.

По итогам оценки всех процессов аудитов, выполняемых в строгом соответствии с программой аудита ИСМ, заполняется следующая матрица (таблица 2).

Таблица 2. Схема размещения результатов аудита процессов ИБ

Аудит / Процесс	1	2	…	k
PR_1	PKI_{11}	PKI_{12}		PKI_{1k}
PR_2	PKI_{21}	PKI_{22}		PKI_{2k}
…	…	…	…	…
PR_i	PKI_{i1}	PKI_{i2}		PKI_{ik}

5. Базовый оптимизационный цикл программы аудита ИСМ. На основании имеющихся стандартов аудита (в частности [18]), отраслевых методик (СТО ИББС БР, СТО Газпром СОИБ и пр.), предложим метод многошаговой оптимизации процесса аудита ИСМ для сложных промышленных объектов (СлПО), который позволяет обеспечить систему координации, распределения ресурсов и оперативного доведения результатов аудитов ИСМ до ЛПР. Предложенный метод обеспечивает целенаправленное оперативное функционирование подсистемы ИБ в составе ИСМ и отличается от существующих методов проведением циклической непрерывной оценки результативности R_{ISMS} на основе оптимальной системы

численных показателей (метрик) ИБ { PKI_{ik} }. Предложенный метод состоит из 2-х связанных циклов оптимизации программы аудита ИСМ, отличающихся наличием новых блоков:

1. Базового оптимизационного цикла, который характеризует эффективное выполнение аудита ИСМ в терминах оценки результативности для каждого PR_i-процесса ИБ и каждой PKI_j– метрики ИБ, а также определяет параметры циклов оптимизации ресурсов в программе аудита: глубину ("*scope*"), размер аудиторской выборки, количество привлекаемых аудиторов (экспертов) и пр.

2. Быстрого блока оценки результативности мер коррекции и корректирующих действий в текущем k-м аудите, затрагивающие изменения как следующего процесса ИБ, так и следующего в программе (k+1)-го аудита. Также обеспечивается быстрый переход к оценке показателей результативности ИСМ RISMS в k-м аудите и (k+1)-го аудите для постоянной и оперативной оптимизации всей программы аудита ИСМ.

Рассмотрим базовый оптимизационный цикл программы аудита ИСМ, построенный с учетом формальных требований стандартов ISO по аудиту, стандартов ISAGO, стандартов СТО Газпром и СТО БР ИББС и дополненных новыми компонентами (рисунок 1):

– Формирование оценок результативности по каждому k-му аудиту.

– Формирование быстрой оценки результативности коррекции (корректирующих действий).

– Формирование быстрой обратной связи в текущем цикле аудита.

– Формирование реакции системы — «устрожения» и (или) «смягчения» в зависимости от ИО в текущем цикле аудита.

– Формирование ИО защищенности ИСМ.

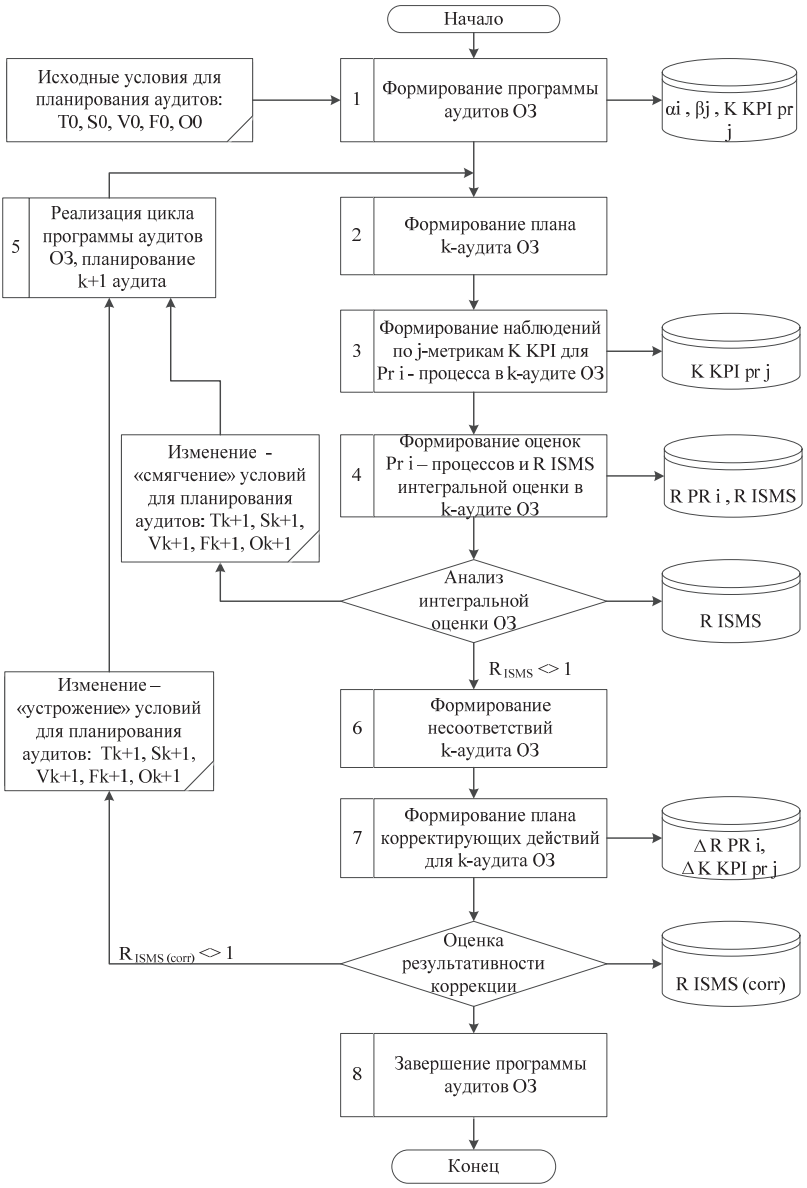

Рис. 1. Базовый оптимизационный цикл программы аудита ИСМ

Определены предусловия (входные данные) для старта базового оптимизационного цикла программы аудита:

- T_0 — базовый период аудитов ИБ.
- S_0 — базовая (плановая) стоимость аудитов ИБ.
- V_0 — базовый объем аудитов ИБ (количество подразделений);
- F_0 — базовый перечень функциональных вопросов аудитов ИБ;
- O_0 — базовый перечень посещаемых объектов аудитов ИБ.

Описание базового оптимизационного цикла программы аудита ИСМ представлено далее по основным шагам.

Шаг 1. Формирование программы аудита, оценивается $R_{ISMS} \geq R_{ISMS\ tar}$ (в соответствии с (1) и (2)). В результате определяются:

- α — весовой коэффициент для групповой метрики процесса ИБ;
- β — весовой коэффициент для частной метрики процесса ИБ;
- k — количество аудитов ИБ в программе аудита;
- R_{ISMS} — текущая ИО результативности СМИБ;
- $R_{ISMS\ tar}$ — целевая ИО результативности СМИБ;
- γ — количество аудитов в программе аудита;
- Δ — допустимая «невязка» показателя $R_{\mathbf{ISMS\ tar}}$;
- $K_{PR\ i}$ — целевой показатель результативности *i*-процесса;
- $K_{KPI\ j}$ — целевой показатель результативности *j*-метрики для *i*-процесса.

Шаг 2. Формирование плана k-го аудита. В результате утверждается план k-го аудита.

Шаг 3. Выполнение k-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 4. Выполняется сбор наблюдений по итогам k-го аудита, соответственно $K_{PR\ i}$ и $K_{KPI\ j}$. В результате заполняется база данных аудита показателями $K_{PR\ i}$ и $K_{KPI\ j.}$

Шаг 5. Выполняется формирование оценки R_{ISMS} — интегральной оценки на k-м аудите. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 6. Выполняется оценка степени достижения R_{ISMS} по итогам k-го аудита целевого показателя $R_{ISMS\ tar}$. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 7. В случае, если $R_{ISMS} \geq R_{ISMS\ tar}$, т.е. достигается установленный показатель результативности, выполняется информирование руководителя программы аудита о возможном «смягчении» условий планирования (k+1)-го аудита. В частности, могут быть снижены частота или объем программы аудита, что, соответственно, снизит и затраты на выполнение аудитов. Далее переход на шаг 13 к реализации (продолжению) программы аудита,

выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае, если $R_{ISMS} < R_{ISMS\ tar}$, т.е. не достигает установленный показатель результативности, выполняется формирование перечня несоответствий на k-м аудите. Выполнение далее (k+1)-го аудита может быть приостановлено по решению руководителя программы аудита с целью снижения расходов. В результате формируется отчет по итогам k-го аудита.

Шаг 9. На основании сформированного перечня несоответствий на предыдущем шаге формируется план коррекции и корректирующих действий для выявленных несоответствий на k-м аудите. В результате выполняется заполнение базы данных аудита показателями, соответственно, ΔK_{PRi} и ΔK_{KPIj} для k-го аудита, который характеризует степени отклонения, соответственно, по целевому показателю PR_i-процесса ИБ в целом и $K_{KPI\ j}$ по отдельным (частным показателям).

Шаг 10. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-го аудита.

Шаг 11. В случае, если $R_{ISMS\ (corr)} \geq R_{ISMS\ tar}$, т.е. достигается полностью установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование руководителя программы аудита и в случае отсутствия иных несоответствий за период реализации корректирующих мер — завершение программы аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае, если $R_{ISMS\ (corr)} < R_{ISMS\ tar}$, т.е. не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR *i*-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 13 к реализации (продолжению) программы аудита, выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 13. В случае, если подтверждена результативность корректирующих мер для всех выявленных несоответствий на k-го аудите, выполняется переход к дальнейшей реализации (продолжении) программы аудита и выполнению (k+1)-го аудита.

6. Быстрый блок оценки результативности программы аудита ИСМ. Быстрый блок оценки результативности мер коррекции и корректирующих действий в текущем k-м аудите, определяющий изменения как следующего процесса, так и следующего в

программе (k+1)-го аудита, а также же быстрый переход к оценке показателей результативности СМИБ представлены на рисунке 2.

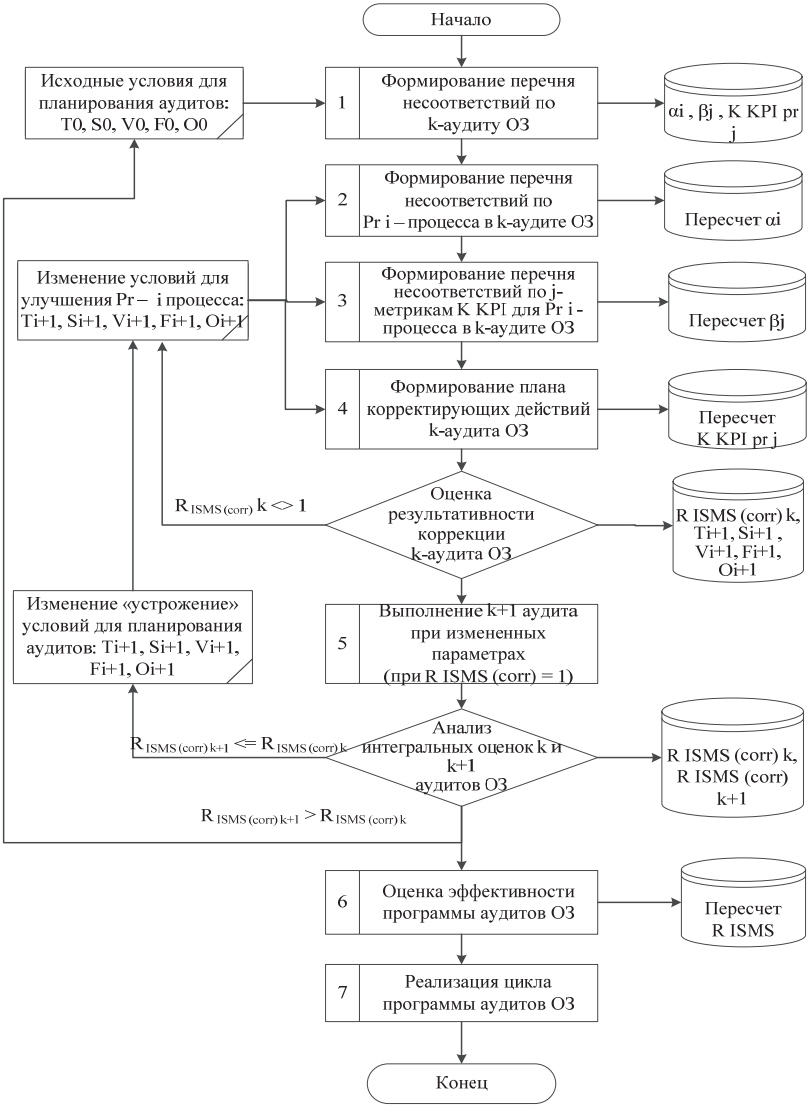

Рис. 2. Быстрый блок оценки результативности программы аудита ИСМ

Описание быстрого блока оценки результативности программы аудита ИСМ представлено далее по основным шагам.

Шаг 1. Формирование программы аудита. В результате определяются:

- α — весовой коэффициент для групповой метрики процесса ИБ;
- β — весовой коэффициент для частной метрики процесса ИБ;
- k — количество аудитов ИБ в программе аудита ОЗ;
- RISMS — текущая ИО результативности СМИБ;
- RISMS tar — целевая ИО результативности СМИБ;
- γ — количество аудитов в программе аудитов;
- Δ — допустимая «невязка» показателя RISMS tar;
- KPR i — целевой показатель результативности j-процесса;
- $K_{KPI\,j}$ — целевой показатель результативности *i*-метрики для *j*-процесса.

Шаг 2. В случае выявленных несоответствий по установленным (базовым) критериям аудита, формируется перечень несоответствий k-го аудита. В результате формируется перечень несоответствий k-го аудита.

Шаг 3. Каждое выявленное несоответствие последовательно соотносится с определенным PR*i*-процессом ИБ. В результате выполняется пересчет весовых коэффициентов (групповых) α PR *i*-процессов ИБ. Заполнение базы данных аудита новым показателем α.

Шаг 4. Каждое выявленное несоответствие последовательно соотносится с j-метрикой и показателем K_{PRi} по определенному PR*i*-процессу ИБ. В результате выполняется пересчет весовых коэффициентов (частных) β для метрик PR*i*-процессов ИБ. Заполнение базы данных аудита новым показателем β.

Шаг 5. Выполняется формирование плана корректирующих действий по k-му аудиту. В результате выполняется пересчет PR*i*– целевого показатель результативности *i* –го процесса. Заполнение базы данных аудита новым показателем $K_{PR\,i.}$

Шаг 6. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-аудита и новыми значениями T_j , S_j , V_j , F_j , O_j.

Шаг 7. В случае, если $R_{ISMS\ (corr)} < R_{\ ISMS\ tar}$, т.е. для k-аудита не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности,

могут быть увеличены частота или объем программы аудита для тех PR_j-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае если $R_{ISMS\ (corr)} \geq R_{\ ISMS\ tar}$, т.е. для k-го аудита достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется реализация следующего по программе аудитов: (k+1)-го аудита с учетом новых измененных параметров по итогам успешной реализации корректирующих действий по предыдущему k-му аудиту. В результате формируется отчет по итогам k-го аудита.

Шаг 9. Выполняется анализ интегральных оценок для k и (k+1) аудитов соответственно: $R_{ISMS\ (corr)\ k}$, и $R_{ISMS\ (corr)\ k+1}$. В результате заполняется база данных аудита показателем R_{ISMS} (corr) k для k-го аудита и R_{ISMS} (corr) k+1 для (k+1)-го аудита.

Шаг 10. В случае если $R_{ISMS\ (corr)\ k+1} <= R_{ISMS\ (corr)\ k,}$ выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR_j-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 11. В случае если $R_{ISMS\ (corr)\ k+1} > R_{ISMS\ (corr)\ k}$, выполняется информирование руководителя программы аудита о возможном возврате к базовым условиям планирования аудита. Далее переход на шаг 5 к формированию плана корректирующих действий для (k+1)-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае повышения уровня результативности программы $R_{ISMS\ (corr)\ k+1} > R_{ISMS\ (corr)k}$ выполняется оценка программы аудита в целом, в том числе в экономическом аспекте (минимизация S-параметра). В результате формируется отчет по итогам k-го аудита.

7. Заключение. Предложенная методика оптимизации программы аудита ИСМ основана на современных риск-ориентированных стандартах и позволяет обеспечить постоянную

оптимизацию процесса выполнения проверок (аудитов) ИБ на основе гибких связанных адаптивных алгоритмов. Экспериментальная проверка предложенной методики проведена в период 2014–2016 гг. при выполнении проектов ООО «Газинформсервис» (имеется акт внедрения). Применение указанных конкретных блоков оптимизации в методике для иных ИСМ может, вероятно, потребовать иных параметров (например, при выборе в качестве критериев иных отраслевых стандартов или иного количества и состава векторного аргумента оптимизации).

Литература

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems // Requirements, International Organization for Standardization. 2013. 23 p.
2. ISO 55000:2014 Asset management – Overview, principles and terminology // International Organization for Standardization. 2014. 19 p.
3. ISO 55001:2014 Asset management – Management systems – Requirements // International Organization for Standardization. 2014. 14 p.
4. ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001 // International Organization for Standardization. 2014. 32 p.
5. PAS-99:2012 «Specification of common management system requirements as a framework for integration» // International Organization for Standardization. 2012. 36 p.
6. *Шишкин В.М., Юсупов Р.М.* Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. 2002. Вып. 1. №. 1. С. 65–78.
7. *Юсупов Р. М., Шишкин В. М.* О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. 2008. Вып. 6. С. 39–59.
8. *Котенко И.В., Саенко И.Б., Юсупов Р.М.* Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) // Труды СПИИРАН. 2010. Вып. 2. С. 226–248.
9. *Лившиц И.И., Полещук А.В.* Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром // Труды СПИИРАН. 2015. № 3. С. 33–44.
10. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 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. Вып. 6. С. 72–94.
12. *Арзамазов М.А., Серов Г.П.* Консолидация общих требований стандартов к отдельным системам менеджмента и инновации при разработке интегрированных систем менеджмента // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. 2012. № 1. С. 52–55.
13. *Малышева Е.Ю., Бобровский С.М.* Архитектура информационной системы оценки интегрированных систем менеджмента // Вектор науки Тольяттинского государственного университета. 2012. № 1. С. 64–67.
14. *Ajam M., Alshawi M., Mezher T.* Augmented process model for e-tendering: toward integrating object models with document management systems // Automation in Construction. 2010. vol. 19. no. 6. pp. 762–778.

15. *Шеверда В.В.* Подходы к разработке интегрированных систем менеджмента на предприятиях электронной промышленности // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2012. № 3. С. 250–254.
16. *Mengersen K., Whittle P.J.L., et al.* Beyond compliance: Project on an Integrated system approach for PEST risl management in South East Asia // EPPO Bulletin. 2012. vol. 42. no. 1. pp. 109–116.
17. *Портянко Т.М.* Тенденции создания интегрированных систем менеджмента на предприятиях промышленного комплекса // Восточно-Европейский журнал передовых технологий. 2010. Т. 2. № 8 (44). С. 40–43.
18. ГОСТ Р ИСО 19011:2011. Руководящие указания по проведению аудитов систем менеджмента // Стандартинформ. 2013. 35 с.
19. *Griffith A.* Management systems for sustainable construction: Integrating Environmental, Quality and Safety management systems // International Journal of Environmental Technology & Management. 2002. vol. 2. no 1–3. pp. 114.
20. RAROC and risk management: Quantifying the risks of business // Bankers Trust New York Corporation. 1995.
21. *Smith G.E.* Auditing statistical methods for ISO 9001 // Transactions of 46th Annual Quality Congress. Milwaukee. WI. 1992. vol. 46. no. 0. QICID: 9905. pp. 849–54.
22. ГОСТ Р ИСО/МЭК 17021:2011. Оценка соответствия. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента // Стандартинформ. 2013. 37 с.
23. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems // Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
24. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems // Measurement, International Organization for Standardization. 2009. 55 p.

Лившиц Илья Иосифович — к-т техн. наук, ведущий аналитик, ООО "Газинформсервис". Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 50. Livshitz.il@yandex.ru; 198188, Санкт-Петербург, а/я 35; р.т.: +7(812) 677-20-50, Факс: +7(812) 677-20-51.

I.I. LIVSHITS

THE OPTIMIZATION METHOD OF THE INTEGRATED MANAGEMENT SYSTEM AUDIT PROGRAM

Livshits I.I. **A Method for Optimizing the Integrated Management System Audit Program.**

Abstract. The application of Integrated Management Systems (IMS) is now attracting the attention of senior management of a variety of organizations: refineries, instrument-making enterprises, aviation enterprises, defense organizations, etc. However, performing ISM audits as a verification of conformance to different ISO standards with a substantial reduction or limitation of available resources remains a major problem.

At the same time, continuous improvement of management principles and, in particular, transition to risk-based thinking provide a greater interest in the rational use of ISO standards. In this article we suggest a technique of optimization of IMS audit program based on principles of continuous adaptation when collecting data during a single audit micro-cycle. An additional advantage of the proposed technique is the use of numerical metrics of IT-security audit, contributing to continuous improvement of the level of IT security in organizations.

Keywords: Information security, Integrated Management System, standard, audit, IT security Management System.

Livshitz Ilya Iosifovich — Ph.D., lead analyst, LLC "Gasinformservice". Research interests: system analyses, IT-security, risk-management. The number of publications — 50. Livshitz.il@yandex.ru; 198188, Saint-Petersburg, a/ja 35; office phone: +7(812) 677-20-50, Fax: +7(812) 677-20-51.

References

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. 23 p.
2. ISO 55000:2014 Asset management – Overview, principles and terminology. International Organization for Standardization. 2014. 19 p.
3. ISO 55001:2014 Asset management – Management systems – Requirements. International Organization for Standardization. 2014. 14 p.
4. ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001. International Organization for Standardization. 2014. 32 p.
5. PAS-99:2012 «Specification of common management system requirements as a framework for integration». International Organization for Standardization. 2012. 36 p.
6. Shishkin V., Yusupov R.M. ["The Doctrine of information security of Russian Federation" — an experience of quantitative modeling]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2002. vol. 1. no.1. pp. 65–78. (In Russ).
7. Yusupov R.M., Shishkin V. [About some contradictions in the decision of information security problems]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2008. vol. 6. pp. 39–59. (In Russ).
8. Kotenko I.V., Saenko I.B., Yusupov R.M. [Analytical review of the reports of the International Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA&PS4CS 2010)]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2010, vol. 2(13). pp. 226–248. (In Russ).
9. Livshits I., Poleshuk A. [Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 3(40). pp. 33–44. (In Russ).

10. Livshitz I. [Practical purpose methods for ISMS evaluation]. *Menedzhment kachestva – Quality Management*. 2013. vol. 1. pp. 22–34. (In Russ).
11. Livshitz I. [Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – airport complexes]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2014. vol. 6, pp. 72–94. (In Russ).
12. Arzamazov M.A., Serov G.P. [Consolidation of the general requirements of standards to individual management systems and innovation in the development of integrated management systems]. *Nauka I technologii truboprovodnogo transporta nefti I nefteproduktov – Science and Technologies oil and oil products pipeline transportation*. 2012. vol. 1. pp. 52–55. (In Russ).
13. Malysheva E.Y., Bobrovski' S.M. [The architecture of the information system of integrated management systems assessment]. *Vektor nauki Tol'atti Universitet – Vector Science Togliatti State University*. 2012. vol. 1. pp. 64–67. (In Russ).
14. Ajam M., Alshawi M., Mezher T. Augmented process model for e-tendering: toward integrating object models with document management systems. Automation in Construction. 2010. vol. 19. no 6. pp. 762–778.
15. Sheverda V.V. [Approaches to the development of integrated management systems for the electronics industry companies]. *Voprosy sovremennoy nauki i praktiki – Questions of modern science and practice*. 2012. vol. 3. pp. 250–254. (In Russ).
16. Mengersen K., Whittle P.J.L., et al. Beyond compliance: Project on an Integrated system approach for PEST risl management in South East Asia. EPPO Bulletin. 2012. vol. 42. no 1. pp. 109–116.
17. Portyanko T.M. [Trends in development of integrated management systems at the enterprises of the industrial complex]. *Vostochno-Evrope'ski' zhurnal peredovyh technologi'– Eastern European advanced technology magazine*. 2010. vol. 8 (44). pp. 40–43. (In Russ).
18. GOST 19011:2011. [Guidelines for auditing management systems]. Standartinform. 2013. 35 p. (In Russ).
19. Griffith A. Management systems for sustainable construction: Integrating Environmental, Quality and Safety management systems. International Journal of Environmental Technology & Management. 2002. vol. 2. no 1–3. pp. 114.
20. RAROC and risk management: Quantifying the risks of business. Bankers Trust New York Corporation. 1995.
21. Smith G.E. Auditing statistical methods for ISO 9001 // Transactions of 46th Annual Quality Congress. Milwaukee. WI. 1992. vol. 46. no. 0. QICID: 9905. pp. 849–54.
22. GOST R 17021:2011. [Conformity assessment -Requirements for bodies providing audit and certification of management systems]. Standartinform. 2013. 37 p. (In Russ).
23. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
24. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization. 2009. 55 p.