УДК 004.94

И.И. Лившиц

ПРИМЕНЕНИЕ МОДЕЛИ СМИБ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ МЕНЕДЖМЕНТА

Лившиц И.И. **Применение моделей СМИБ для оценки защищённости интегрированных систем менеджмента.**

Аннотация. При создании современных систем менеджмента, в том числе – интегрированных систем менеджмента (ИСМ) необходимо решать комплекс вопросов обеспечения безопасности основных бизнес-процессов организации. Приоритет направления безопасности, особенно информационной безопасности (ИБ) постоянно возрастает в силу усиления конкурентной среды, появления новых угроз и значительной сложности выполнения процедур риск-менеджмента. Для ИСМ весьма актуальна проблема получения оценки защищенности, что позволяет в краткосрочном и/или прогнозном аспектах оценить присущие данной организации риски, спроектировать эффективную систему менеджмента информационной безопасности (СМИБ) и внедрить экономически обоснованные средства обеспечения безопасности. В предлагаемой работе предложены некоторые подходы для создания модели оценки защищенности ИСМ в соответствии с требованиями стандарта ISO/IEC 27001:2005 и ISO 22301:2012. Учитывая относительную новизну данных стандартов в практическом применении к исследуемой проблеме в ИСМ, предлагаемые подходы могут быть полезны при планировании СМИБ, оценке защищенности уже созданных ИСМ, а также, в частности, для решения практических задач – аудитов ИБ в организациях.

Ключевые слова: активы, информационная безопасность (ИБ), интегрированная система менеджмента (ИСМ), стандарт, система менеджмента информационной безопасности (СМИБ), уязвимости, угрозы, риски, менеджмент рисков.

Livshitz I.I. **The practice of security assessment for Integrated Management Systems (IMS) based on the ISMS models.**

Abstract. While a modern management systems creating (include - Integrated Management Systems, IMS), the range of security aspects for core business processes of the organization should be solved. Priority areas of security, especially information security (IS) is increasing due to gain the competitive environment, the emergence of new threats and the considerable complexity of the risk management procedures. IMS is highly relevant to the problem of obtaining security assessment, allowing the short and / or evaluate the prognostic aspects inherent in the organization's risks, to design an effectiveness information security management system (ISMS) and implement efficiency reasonable security measures. In this issue proposed some approaches to creating a models for IMS security assessment in accordance with the requirements both of ISO / IEC 27001:2005 and ISO 22301:2012. Given the relative newness of these standards in the practical application to the research problem in the ISM, the proposed approaches can be useful in the planning of the ISMS, security assessment has created IMS, and, in particular, to solve practical problems – IT-security audits in organizations.

Keywords: assets, IT-security, Integrated Management System (IMS), standard, IT-security management system (ISMS), security controls, threat, vulnerability, risk, risk-management.

1. Введение. При создании интегрированных систем менеджмента (ИСМ), состоящих минимально из 2-х и более систем менеджмента (например, системы менеджмента информационной безопасности (СМИБ) и системы управления услуг (СУУ)), во внимание принимается широкий спектр требований, важнейшими из которых являются требования непрерывности и устойчивости бизнес-процессов организации. В этом процессе высшее руководство организации может принимать как «базовую» точку методологии для анализа различных стандартов в составе ИСМ, содержащих требования в части, касающейся обеспечения безопасности бизнес-процессов в широком толковании этого термина. Прежде всего, это международные стандарты серии ISO 9000, ISO/IEC серии 27000 и ISO/IEC серии 20000. Известно, что при создании современных ИСМ, помимо известных проблем кооперации требований различных систем менеджмента, необходимо обеспечить «интегральное соответствие» требованиям бизнеса – прежде всего экономической эффективности по целевой функции достижения прибыли и минимизации издержек и, как не менее значимой вложенной задачи – формального соответствия законодательным требованиям различных регуляторов (т.н. «***compliance***», например, ФЗ-63 «Об электронной подписи», ФЗ-152 «О персональных данных», ФЗ-161 «О национальной платежной системе»).

2. Постановка задачи. Оценку защищённости ИСМ предлагается формировать на чёткой парадигме «целевого» стандарта ISO/IEC 27001:2005 (далее *Стандарта*): «Бизнес» - «Активы» - «Уязвимости» - «Угрозы» - «Риски» - «Средства защиты». Для полноты комплексной оценки ИСМ в качестве сущностей иерархической модели СМИБ могут быть востребованы также стандарты ISO/IEC серии 20000 – устанавливающие требования к СУУ и стандарты серии ISO 22301 – устанавливающие требования к системам менеджмента непрерывности бизнеса (СМНБ). С учетом сказанного выше, основная методологическая роль в оценке защищённости ИСМ возлагается на модель СМИБ (созданная по требованиям *Стандарта*).

Кратко рассмотрим несколько основополагающих понятий СМИБ, которые будут полезны для корректного восприятия предложенной модели и методов оценки защищённости ИСМ, применительно к целям данной публикации. В Стандарте применяются понятия «Политика ИБ», «Область сертификации» и «Заявление о применимости» (см. пункт 4.2.1). Кратко взаимосвязь

этих основных понятий СМИБ может быть представлена следующим образом (см. рис.1).

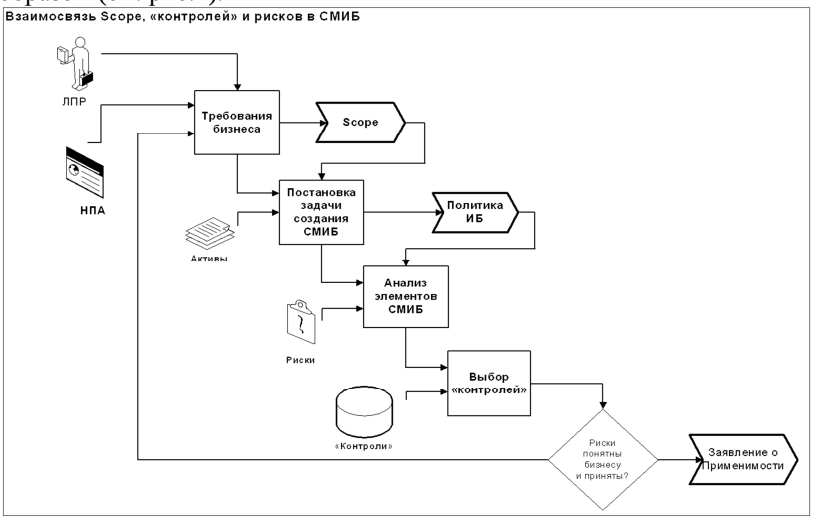

Рис. 1. Взаимосвязь Scope, средств обеспечения безопасности» и рисков в СМИБ.

По представленной постановке задачи необходимо дать краткие комментарии:

- В любой организации используются активы, т.е. экономические сущности, которые вовлечены в процесс создания продукции (СМК) и/или услуг (СУУ) и служат для получения дохода, следовательно, должны быть защищены;
- Любые активы имеют уязвимости, следовательно, существуют угрозы и риски утраты целостности, доступности и /или конфиденциальности данных активов организации (СМИБ);
- На практике ценные активы организации не всегда должным образом определены, категорированы, оценены и защищены; менее вероятно, что реализована система ИБ, и еще менее вероятно, что система ИБ сертифицирована или оценена каким-либо достоверным и объективным способом (минимально – в рамках внутренних аудитов ИБ);
- Одна из ключевых проблем – оценка защищённости активов организации, которая дает высшему руководству сопоставимые, достоверные, оперативные и корректные данные [4].

3. Предпосылки для разработки модели СМИБ. В последнее время появились новые виды угрозы, воздействие которых (***impact***, ущерб, негативное влияние) чрезвычайно опасно:

- Совершенствование атак. Исследования (Positive Hack Days 2012) показали, что атаки на хэш-функции паролей вполне успешны (хэши паролей LinkedIn хранились без использования «соли»). Наиболее уязвимыми оказались хэши MD5, SHA1 и MySQL5. Как показало исследование SplashData, до сих пор используются пароли «password» и «123456».
- Угрозы широкого применения «кибероружия» (появление функционала банковского «троянца» в Gauss и Flame), способное собирать и передавать историю посещаемых сайтов и пароли, используемые в онлайн-сервисах. По данным системы мониторинга Kaspersky Security Network, обнаружено воздействие Gauss на клиентов Citibank и системы PayPal.
- Угрозы нарушения функционирования критичных систем. Экспертами Digital Security была продемонстрирована атака на ERP-систему SAP, представляющая собой последовательную эксплуатацию уязвимостей: НСД к веб-сервису модуля SAPPI, XML Tunneling и переполнение буфера в SAP Kernel. Вся атака поместилась в один XML-пакет, который практически ни одна IDS-система не определила бы как вредоносное ПО.
- Угрозы коммерческого подкупа должностных лиц. По данным компании HeadHunter, каждый 4-й опрошенный, признался, что хотя бы раз в жизни соглашался на «откат» как вид взятки. При этом средняя сумма откатов составила свыше 200 тысяч руб. Как показал опрос, 15% респондентов готовы к откату, если предложат.
- Угрозы утечки чувствительной информации. По данным Zecurion Analytics, оценка издержек только на ликвидацию последствий утечки информации о пластиковых картах клиентов компании Global Payments составила $84,4 млн. Кроме того, компания ожидает списать на расходы по ликвидации последствий утечки в следующем году еще до $35 млн. После инцидента крупнейшие платежные системы Visa и MasterCard исключили Global Payments из списка доверенных подрядчиков.
- Угрозы финансовой системе на уровне государства. По опубликованным данным, за 9 месяцев 2012 г. «Сбербанк»

пресек более 5.000 попыток хищения средств физических лиц на сумму более 500 млн. руб., а также свыше 400 попыток хищения средств юридических лиц на сумму более 770 млн. руб. через каналы ДБО. Из этих данных можно сделать вывод о том, что онлайн-банкинг крупнейшей кредитной организации страны подвергается атакам чаще, чем 20 раз в день.

Стандарт предлагает концепцию ИБ, построенную на «триаде безопасности» - **конфиденциальности**, **целостности** и **доступности**, которая, в случае потребности конкретной организации может быть расширена и по иным критериям: ***неотказуемости***, ***надежности***, ***подотчетности*** и пр. (см. п. 3.4). Важно отметить, что в *Стандарте* предлагается комплексный подход, учитывающий различные аспекты ИБ (физический, организационно-административный, технический, юридический и пр.). *Стандарт* содержит универсальные принципы, которые позволяют предоставить независимые оценки СМИБ и, в равной мере, для ИСМ. В процессе анализа (оценки) защищенности ИСМ потребуются все активности цикла PDCA – необходимо постоянно оценивать новые угрозы, проводить детальный анализ защищенности и проводить переоценку состава средств обеспечения ИБ в фокусе рисков.

4. Менеджмент рисков в ИСМ. В процессе разработки, внедрения, эксплуатации и постоянного улучшения ИСМ следующие риски должны быть приняты во внимание:

- неправильное выделение критичных бизнес-процессов – что повышает затраты на реализацию средств защиты в СМИБ и, последовательно – в целом для ИСМ;
- некорректное определение активов, подлежащих защите - что необоснованно повышает экономические затраты – например существенные различия в логических и физических границах для области сертификации (Scope);
- неосведомленность о ценности НМА (в т.ч. информационных активов – лицензий на ПО, что особенно критично для СУУ);
- отсутствие программы внедрения ИСМ (с четкими этапами, целями и сроками, например, применительно к информации, отнесенной в установленном законом РФ порядке к коммерческой тайне по ФЗ-98 и пр.);
- формально разработанные процедуры ИБ (например, регламент аудита ИБ по шаблонам, предоставленным консультантами);

- непринятие во внимание требований обеспечения непрерывности бизнеса (например, в соответствии с требованиями ряда ФЗ и/или требований А.14 *Стандарта*).

5. Известные подходы при оценке защищённости систем менеджмента. Для решения проблемы оценки защищённости в современных организациях применяются различные методики, получившие достаточное распространение за многолетнюю практику использования в различных отраслях [4]. Кратко рассмотрим несколько основных методик:

- Международные стандарты ISO по системам менеджмента, содержащие требования к ИБ (например, СМИБ, СУУ, СМНБ), позволяющие выполнять как внутренние аудиты (первой стороной), так и внешние аудиты (второй и третьей стороной);
- Комплекс СТО БР ИББС (разработка ЦБ РФ на базе стандарта ISO 17799), позволяющий кредитным организациям выполнять самооценку и/или внешнюю оценку по единой количественной методике:
- Аттестация по руководящим документам ФСТЭК РФ (комплекс документов, предназначенный для оценки объектов автоматизации по установленным методикам и классам);
- Оценки по отраслевым стандартам (например, PCI DSS), методикам (например, CobiT5), позволяющим получить оценки соответствия конкретных технологий по специфическим требованиям.

Очевидно, что для целей формирования объективных (и воспроизводимых независимо) оценок защищённости систем менеджмента (минимально – СМИБ, целевая задача – ИСМ), могут быть применены только стандарты ISO, т.к. все прочие методики содержат свои отраслевые требования, которые, в частном конкретном случае, не могут быть оценены (например, требование «*Банковский платежный технологический процесс*» в СТО БР ИББС) в организации ИТ–провайдере или организации – разработчике ПО.

Важно обратить внимание, что общие подходы к интеграции для рассмотренных МС могут быть взяты из ISO/IEC 27013:2012 «Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1».

6. Требования к модели оценки защищённости ИСМ. К модели СМИБ, пригодной для оценки защищённости ИСМ, как показывает

статистика выполненных проектов [4], целесообразно сформировать следующие требования:

- Соответствия области сертификации (***Scope***) ИСМ. Должны быть приняты во внимание размещение инфраструктуры организации, физические и логические границы, требования к персоналу (в том числе на аутсорсинге), применяемые технологии (например, технологии предоставления услуг, в частности через операторскую службу Service Desk).
- Соответствия требованиям к точности. Должна быть предложена модель СМИБ, предоставляющая руководству организации результаты оперативного или прогнозного моделирования с требуемой точностью. Для этого, например, в предлагаемой модели СМИБ могут быть учтены конкретные средства обеспечения ИБ из Приложения «А» Стандарта;
- Соответствия требованиям к адекватности модели. Известно, что модели применяются для понимания структуры и поведения объекта (ИСМ), но без полномасштабного и абсолютно точного его воссоздания со всеми деталями. Таким образом, модель СМИБ должна позволять оценивать уровень ИБ организации с достаточной детализацией (например, по структуре «доменов», «групп» и средств обеспечения ИБ, принимая во внимание, что допускаются исключения из Приложения «А» Стандарта – при соответствующем обосновании рисков);
- Соответствия целям ИСМ. В случае постановки задачи цели создания ИСМ (в составе, как минимум, СУУ и СМИБ), очевидно, необходимо принять во внимание корректность учета входных данных (которые сами по себе уже могут содержать, коммерческую тайну организации, правила допуска работников к отчетам для анализа со стороны высшего руководства).

7. Применение модели СМИБ для оценки защищённости ИСМ. Поставленная проблема может быть решена при развитии «базовой» модели СМИБ (созданной в соответствии с требованиями *Стандарта*) за счет метода анализа иерархий (МАИ), предложенного Т. Саати [1] и дающей возможность применять совместно иерархическую систему критериев ИБ и средств обеспечения ИБ. Суть метода МАИ состоит в том, что выбирается множество альтернатив, множество критериев и цель (как вершина иерархии), далее по каждому элементу иерархии независимыми экспертами (или группами

экспертов) устанавливается относительная степень предпочтения, которая указывает значимость сопоставляемых элементов иерархии для эксперта. Численное значение предпочтения каждого элемента иерархии стандарта определяется их попарным сравнением по шкале отношений (на практике в большинстве случаев применяется целочисленная шкала от 1 до 9).

Предложенное развитие «базовой» по отношению к модели СМИБ позволяет описать процесс создания, внедрения и оптимизации СМИБ таким образом, что общие свойства элементов (средств обеспечения ИБ) рассматриваются в качестве элементов следующего (по иерархии) уровня реальной системы. Далее эти элементы, в свою очередь, могут быть сгруппированы в соответствии с другим набором свойств, создавая последующие элементы иного более высокого уровня, и далее до тех пор, пока не будет достигнут единственный элемент – вершина, которая и является целью решения. Предложенную модель обычно называют иерархией, т. е. системой уровней, каждый из которых состоит из многих элементов, иначе именуемых факторами. Известно, что неравномерность по всему множеству факторов приводит к необходимости определения приоритетов или «весов» факторов [1].

Новизна предлагаемой модели СМИБ по сравнению с «базовой» моделью [4] заключается в совместном применении в качестве всех элементов иерархической структуры МАИ (цели, критериев, факторов, «стандартов») соответствующих сущностей *Стандарта* и расширенных математических правил самопроверки корректности («оценки однородности»), и благодаря этому предоставляющей возможность построения математической модели, пригодной для выполнения быстрой оптимизации СМИБ (в том числе и «базовой» модели) и получения математически корректных численных оценок уровня защищённости основных активов бизнеса.

В предложенной модели СМИБ, построенной на базе модифицированного МАИ относительно «стандартов» реализованы следующие уровни иерархии:

- в качестве цели определена информационная безопасность;
- в качестве критериев верхнего уровня применяется базовая «триада безопасности» – «конфиденциальность», «целостность» и «доступность»;
- в качестве прочих элементов иерархии применяются конкретные средства обеспечения ИБ, Приложения «А» стандарта [3], разделы А.5 – А.15.

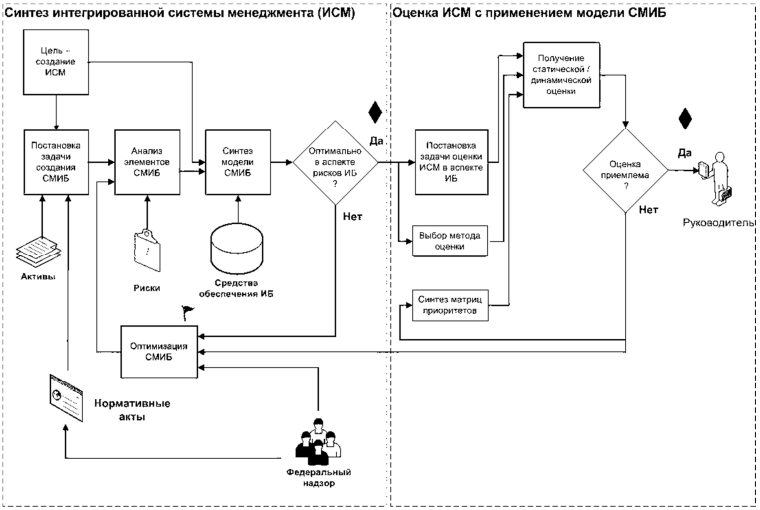

Рис. 2. Метод применения модели СМИБ для ИСМ.

Отличительными свойствами предложенного развития модели СМИБ для ИСМ являются наличие 2-х последовательных контуров управления – «**Синтез**» и «**Оценка**», охваченных обратной связью в функции обеспечения непрерывной оценки пригодности и улучшения СМИБ (напомним, это требование *Стандарта*).

Первый контур («**Синтез**») практически детализирует выполнение требований стандартов, например для ИСМ – PAS 99:2012, и охватывает все основные сущности СМИБ, о которых кратко говорилось ранее. Важным элементом является блок оптимизации, который реализует постоянный контроль адекватности модели СМИБ (в соответствии с классической моделью PDCA) и соответствия внешним нормативным требованиям. На «выходе» первого контура предложенного развития модели СМИБ формируются документированные свидетельства СМИБ (см. п. 4.3.1. *Стандарта*), среди которых обязательные: «Политика ИБ», «Заявление о Применимости», документированные процедуры («Управление документами», «Управление записями», «Управление корректирующими действиями», «Управление предупреждающими действиями», «Внутренние аудиты»), а также документы по менеджменту рисков: точная идентификация активов (реестр), выбор ценных активов, подлежащих защите, выбор методики оценки рисков, формирование плана обработки рисков, подготовка отчетов по оценке рисков (в том числе остаточных рисков).

Во втором контуре («**Оценка**») выполняется оценка ИСМ с применением метрик предложенной модели СМИБ. Этот процесс можно формализовать, приняв за входные данные измеряемые численные показатели (метрики ИБ). В качестве примера нормативных документов, которые содержат метрики ИБ, можно рекомендовать стандарт ISO/IEC 27004, COBIT5, ITIL v.3.1 и пр. На «выходе» второго контура формируются оценки уровня защищённости основных активов бизнеса, например статические (дающие быстрый аналитический срез по статусу «как есть») или динамические (дающие прогнозные значения).

Рассмотрим более подробно выбор методов оценки в предложенной модели СМИБ. Выбор конкретного метода оценки в предложенной модели СМИБ подразумевает возможность применения двух основных методов оценки:

- **Статический метод оценки** – характеризуется формированием оценок для высшего руководства на основании расчета «статических данных», т.е. матрицы векторов приоритетов альтернатив МАИ содержат числа (скаляры) экспертных оценок (как правило, по шкале от 1 до 9) [1];
- **Динамический метод оценки** – характеризуется формированием прогнозов для указанного высшим руководством временного интервала, при этом матрица векторов приоритетов альтернатив МАИ оперирует не числами, а функциями (как правило, нелинейными) [1].

Применение конкретного метода оценки в представленной модели СМИБ может быть реализовано по распоряжению высшего руководства и как «конструирование альтернатив», т.е. использование одного из важнейших преимуществ модифицированного МАИ относительно «стандартов» – предоставление оценок и выбора наилучшей альтернативы в определенном заданном временном интервале прогнозирования [1].

Для расчета динамической оценки по модели СМИБ сформирована матрица предпочтений стандартов (см. Таблицу 1):

Таблица 1. **Динамическая матрица предпочтений стандартов**

	B	**C**	**CH**	**H**
B	1,000	**F1**	**F2**	**F3**
C	**1 / F1**	1,000	**F4**	**F5**
CH	**1 / F2**	**1 / F4**	1,000	**F6**
H	**1 / F3**	**1 / F6**	**1 / F6**	1,000

В качестве функций в результате теоретических прогнозов, подтвержденных в дальнейшем практиков аудитов ИБ [1]-[2] выбраны следующие функции (см. Таблицу 2):

Таблица 2. **Функции для расчета динамической оценки**

Индекс функции	Функция
F1	c_1*exp (c_2*T) + c_3
F2	b_1*Ln (T + b_2) + b_3
F3	a_1* (T) + a_2
F4	d_1*T^2 + d_2*T + d_3
F5	a_1* (T) + a_2
F6	c_1*Exp (T) + c_2

Результаты расчета динамической оценки модели СМИБ представлены на рис. 3 (для переменной T выбран диапазон $-1 \leq T \geq 2$)

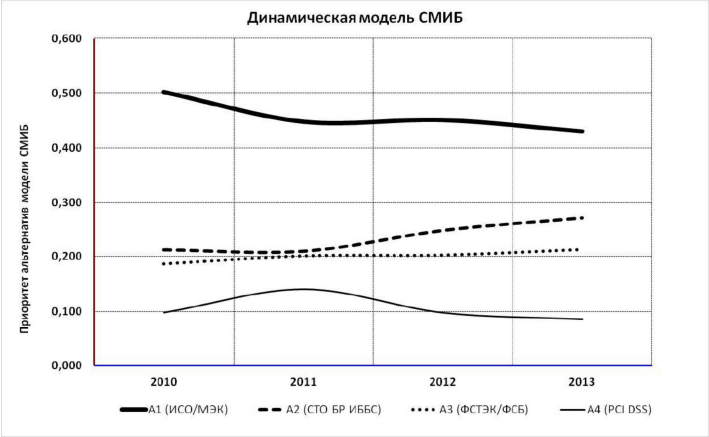

Рис. 3. Расчет динамической модели СМИБ.

В работе [4] представлены краткие результаты применения модели СМИБ (учтены также результаты [2], [3]), которые представлены в Таблице 3.

Таблица 3**. Результаты расчета моделей СМИБ**

	Статическая модель	**Динамическая модель**
Глобальная цель	Оценка защищенности ПДн по модели СМИБ	Оценка защищенности ПДн по модели СМИБ
Альтернативы	Стандарт ISO/IEC 27001:2005; Комплекс СТО БР ИББС; РД ФСТЭК / ФСБ; Стандарт PCI DSS	Стандарт ISO/IEC 27001:2005; Комплекс СТО БР ИББС; РД ФСТЭК / ФСБ; Стандарт PCI DSS
Критерии «верхнего» уровня	Конфиденциальность Целостность Доступность	Конфиденциальность Целостность Доступность
Критерии «нижнего уровня	A.6.1.5 A.7.1.3 A.9.2.4 A.10.1.3	A.6.1.5 A.7.1.3 A.9.2.4 A.10.1.3
Результат расчета	**W = {0,432; 0,217; 0,215; 0,136}^{T}**	**W = {0,448; 0,210; 0,202; 0,141}^{T}** *при T = 0*

Выполнено сравнение результатов расчетов по статической и динамической модели СМИБ – как для определения практической ценности и «качества» предложенной синтезированной модели на базе МАИ относительно стандартов, так и результативности методики оценки защищённости на базе предложенных моделей СМИБ (см. Таблицу 4).

Таблица 4. **Сравнение результаты расчетов модели СМИБ**

Модель / **Альтернатива**	**Статическая**	**Динамическая (при T = 0)**	**Погрешность**	
			Δ	**δ**
A_1 (ИСО/МЭК)	0,432	0,448	0,016	3,53%
A_2 (СТО БР ИББС)	0,217	0,210	0,007	3,45%
A_3 (РД ФСЭК/ФСБ)	0,215	0,202	0,014	6,73%
A_4 (PCI DSS)	0,136	0,141	0,005	3,54%

8. Заключение. Предложенная модель СМИБ имеет ряд преимуществ, свойственных иерархическим структурам, для решения управленческих задач, в том числе для целей оценки защищённости ИСМ:

- Иерархическое представление реальной организации можно использовать для описания влияния изменений приоритетов на верхних уровнях модели на приоритеты элементов нижних уровней (например, для СМИБ изменение состава «триады безопасности», предположим, включение требования «неотказуемости» (non-repudiation), п. 3.4, может влиять на выбор средств обеспечения ИБ).
- Иерархии предоставляют более подробную информацию о структуре и планируемых функциях реальной организации на нижних уровнях и обеспечивают достаточное рассмотрение критериев и целей на высших уровнях (например, в модели СМИБ обеспечивается детальное рассмотрение ряда критериев).
- Реально существующие («практические») системы, модели которых построены с использованием иерархического подхода, рассчитываются намного эффективнее, чем иные типы систем, и допускают быструю модификацию при необходимости (например, с учетом Постановления правительства № 1119);
- Модели, построенные с использованием иерархического подхода, отличаются устойчивостью и гибкостью: устойчивость – малые изменения вызывают столь же малый эффект; и гибкость – добавление элементов к хорошо структурированной иерархии не приводит к нарушению характеристик «базовой» модели.
- Ясный метод вывода результатов оценки – входные данные математически корректны, проходят многоступенчатую оценку, модель имеет точные матричные оценки, выходные результаты объективны, воспроизводимы и «трассируемы» до конкретных средств обеспечения ИБ в Стандарте.
- Не требуется привлечение внешних дорогостоящих консультантов, что позволяет существенно экономить бюджет, кроме того конфиденциальные данные «не уходят» из информационного периметра организации;
- Позволяет получать оценки и проводить независимое сопоставление с лучшими рекомендациями по отрасли – бенчмаркинг (например, взяв за шкалу оценки методику СТО БР ИББС).

9. Выводы. Применение модели СМИБ для оценки защищённости ИСМ с использованием предложенной модели на базе

стандарта ISO/IEC 27001:2005 будет способствовать значительному упрощению процесса создания результативных современных ИСМ (в составе СМИБ и иных систем менеджмента - СУУ, СМНБ), благодаря следующим факторам:

- модели СМИБ позволяют получать оперативные и достоверные оценки уровня защищённости ИСМ исходя из внедренных и/или планируемых средств обеспечения ИБ, повысить объективность и корректность оценки защищённости, сократить сроки реализации проектов создания ИСМ;
- накапливаемые результаты оценок защищённости могут быть использованы для долгосрочного стратегического анализа, снижения издержек при проведении последующих аудитов СМИБ (ИСМ), эффективного обучения персонала, а также для поддержки принятия решений по адекватному выбору технических и/или административных мер для защиты ценных активов организаций;
- применение модели СМИБ позволит учесть и обеспечить стабильность бизнеса современной организации, учесть риски операционной деятельности (в том числе риски ИТ и ИБ при изменении ряда ключевых аспектов – персонал, ввод/вывод активов, ввод/вывод новых средств ИБ и пр.).

Литература

1. *Лившиц И.* Аудит информационной безопасности. Современная практика от ведущего эксперта // Управление качеством. 2011. № 6. С. 46–51.
2. *Лившиц И.* Методы оценки защищенности систем менеджмента информационной безопасности, разработанных в соответствии с требованиями международного стандарта ISO/IEC 27001:2005, автореф. дисс. канд. техн. наук. Санкт-Петербург, 2012. 20 с.
3. *Лившиц И.* Современная практика аудита информационной безопасности // Управление качеством. 2011. № 7. С. 34–41.
4. *Саати Т.* Принятие решений. Метод анализа иерархии. М.: Радио и связь, 1989.

Лившиц Илья Иосифович — к.т.н.; аудитор «ИТСК». Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 28. Livshitz_il@Hotbox.ru; Россия, г. Санкт-Петербург; тел.: +7 812 934-48-46. Научный руководитель — А.А. Молдовян.

Livshitz Ilya — Ph.D.; auditor, ITSK. Research interests: system analyses, IT-security, risk-management. The number of publications — 28. Livshitz_il@Hotbox.ru; Russia, St. Petersburg, phone: +7 812 934-48-46. Scientific advisor — A.A. Moldovyan.

Рекомендовано лабораторией проблем информационной безопасности, заведующий лабораторией Молдовян А.А., д.т.н., проф.
Статья поступила в редакцию 27.08.2013.

РЕФЕРАТ

Лившиц И.И. **Применение моделей СМИБ для оценки защищённости интегрированных систем менеджмента.**

При создании ИСМ, состоящих минимально из 2-х и более систем менеджмента (например, СМИБ и СУУ), во внимание принимается широкий спектр требований, важнейшими из которых являются требования непрерывности и устойчивости бизнес-процессов организации. В этом процессе высшее руководство организации может принимать как «базовую» точку методологии для анализа различных стандартов в составе ИСМ – прежде всего, серии ISO 9000, ISO/IEC серии 27000 и ISO/IEC серии 20000.

В процессе разработки, внедрения, эксплуатации и постоянного улучшения ИСМ должны быть приняты во внимание следующие риски:

- неправильное выделение критичных бизнес-процессов;
- некорректное определение активов, подлежащих защите;
- неосведомленность о ценности НМА;
- отсутствие программы внедрения;
- формально разработанные процедуры ИБ;
- непринятие во внимание требований обеспечения непрерывности бизнеса.

К модели СМИБ, пригодной для оценки защищённости ИСМ, целесообразно сформировать следующие требования:

- Соответствия области сертификации ИСМ;
- Соответствия требованиям к точности;
- Соответствия требованиям к адекватности модели;
- Соответствия целям ИСМ.

Поставленная проблема может быть решена при развитии «базовой» модели СМИБ за счет метода анализа иерархий (МАИ), предложенного Т. Саати и дающего возможность применять совместно иерархическую систему критериев ИБ и средств обеспечения ИБ. Новизна предлагаемой модели СМИБ по сравнению с «базовой» моделью заключается в совместном применении в качестве всех элементов иерархической структуры МАИ (цели, критериев, факторов, «стандартов») соответствующих сущностей Стандарта и расширенных математических правил самопроверки корректности («оценки однородности»).

Применение модели СМИБ для оценки защищённости ИСМ с использованием предложенной модели на базе стандарта ISO/IEC 27001:2005 будет способствовать значительному упрощению процесса создания результативных современных ИСМ, благодаря следующим факторам:

- Модели СМИБ позволяют получать оперативные и достоверные оценки уровня защищённости ИСМ;
- Накапливаемые результаты оценок защищённости могут быть использованы для долгосрочного стратегического анализа;
- Применение модели СМИБ позволит обеспечить стабильность бизнеса современной организации и учесть риски операционной деятельности.

SUMMARY

Livshitz I.I. **The practice of security assessment for Integrated Management Systems (IMS) based on the ISMS models**

When creating IMS consisting of a minimum of 2 or more management systems (such as ISMS and SMS), is taken into account a wide range of requirements, the most important of which is the requirement of continuity and stability of the organization's business processes. TOP-management can take both "basic" point methodology for the analysis of different standards in the IMS- first of all, ISO 9000, ISO / IEC 27000 series and ISO / IEC 20000 series.

In the process of development, implementation, maintenance and continuous improvement of IMS should be taken into account the following risks:

- Improper allocation of critical business processes;
- The incorrect definition of an asset to be protected;
- Lack of awareness of the value of intangible assets;
- The lack of implementation of the program;
- Formal procedures in place IT-Security;
- The failure to take into account the requirements of BCP.

On the model of the ISMS suitable for IMS security assessment, it is appropriate to form the following requirements:

- Conformity certification of IMS;
- Compliance requirements for accuracy;
- Conformance to the adequacy of the model;
- Relevance to the objectives of IMS.

The stated problem can be solved with the development of the "base" model of the ISMS through the analytic hierarchy process (AHP) proposed by T. Saaty and giving the opportunity to be co-hierarchical system of criteria IT-security means to ensure IT- security. The novelty of the proposed model of the ISMS compared to the "base" model is a joint application as all elements of the hierarchical structure of the AHP (objectives, criteria and factors that "standards") of the relevant entities of the Standard and extended self-test the correctness of mathematical rules.

The practice of ISMS models to assess the security for a IMS using the proposed model based on the standard ISO / IEC 27001:2005 will significantly simplify the process of creating a successful modern ISM, due to the following factors:

- Models ISMS can receive prompt and accurate assessment of the level of security of the IMS;
- Accumulating security assessments can be used for long-term strategic analysis;
- Application of the model ISMS will ensure the stability of the modern business organization and consider the risks of operating performance.