УДК 004.94

И.И. Лившиц, А.В. Полещук

ПРАКТИЧЕСКАЯ ОЦЕНКА РЕЗУЛЬТАТИВНОСТИ СМИБ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РАЗЛИЧНЫХ СИСТЕМ СТАНДАРТИЗАЦИИ – ИСО 27001 И СТО ГАЗПРОМ

Лившиц И.И., Полещук А.В. **Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром.**

Аннотация. В данной публикации кратко рассмотрена оценка результативности систем менеджмента информационной безопасности (СМИБ) в соответствии с требованиями различных систем стандартизации, например ГОСТ Р ИСО/МЭК серии 27001 и Системы обеспечения информационной безопасности СТО Газпром серии 4.2 (СОИБ). Данная проблема имеет важное значение для минимизации рисков нарушения ИБ и обеспечения стабильности процессов обработки информации. Обращено внимание на методические сложности совмещения требований различных систем стандартизации (ГОСТ Р ИСО/МЭК и СОИБ), которые необходимо учитывать при оценке постоянного улучшения результативности СМИБ. Предложены формулы для расчета результативности СМИБ и рассмотрены практические примеры (кейсы), поясняющие расчет для конкретных ситуаций. Данные результаты могут найти применение при создании моделей и методов обеспечения аудитов СМИБ и мониторинга состояния объектов, находящихся под воздействием угроз нарушения ИБ, а также при создании моделей и методов оценки защищенности информации и ИБ объектов СМИБ и/или СОИБ Газпром.

Ключевые слова: система менеджмента информационной безопасности (СМИБ), система обеспечения информационной безопасности (СОИБ), метрики ИБ, объект защиты (ОЗ), меры (средства) информационной безопасности.

Livshits I.I., Poleshuk A.V. **Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.**

Abstract. This issue briefly covers the need of numerical evaluation for Information Security Management Systems (ISMS) effectiveness in accordance with the requirements of two or more different standardization systems, such as ISO / IEC 27001 series of standards and Information Security Providing System STO Gazprom series 4.2 (ISPS). This problem is important to minimize the violation of IT-security risks and ensure the information processes stability in the information systems. This issue describes methodological difficulties in reconciling the requirements of different Standardization systems both ISO / IEC and ISPS that must be considered when assessing the ISMS effectiveness. The formulas have been proposed to solve the problem for calculating the ISMS effectiveness and discussed practical examples (cases), explaining the calculation for specific situations. These results can be used to create models and methods to provide the ISMS audits and monitoring IT-security facilities both ISMS and / or ISPS Gazprom.

Keywords: Information Security Management System (ISMS), Information security providing system (ISPS), metrics, object of protection (ObP), controls.

1. Введение. Проблема оценки результативности СМИБ в соответствии с требованиями стандартов ГОСТ Р ИСО/МЭК серии 27001 [1–2] является достаточно известной. Значительно более

сложной проблемой является обеспечение постоянного улучшения результативности СМИБ, созданной с учетом дополнительных отраслевых стандартов (например, СОИБ Газпром [4 – 9]). Решение поставленной выше проблемы может быть затруднено объективными различиями в требованиях СОИБ, которые могут усложнить успешное внедрение СМИБ (например, различия в понятиях «актив» и «объект защиты»). В равной мере это относится и к требованиям по менеджменту рисков [2], а также правилам проведения аудитов в соответствии со стандартом ИСО серии 19011 [3]. В случае, когда высшее руководство организации принимает решение о внедрении и подготовке СМИБ к внешнему аудиту, представляется необходимым проанализировать требования текущей реализации СОИБ (оценить уровень, на котором они реализованы) и выработать решение о комплексе мероприятий, которые следует предпринять для целей обеспечения соответствия СМИБ требованиям стандарта [1]. Одним из важнейших требований, включенных в цикл PDCA, является требование повышения результативности (см. п. 7.1, 8.1 стандарта [1]). Эти оценки должны быть представлены высшему руководству (ЛПР) для принятия адекватных («разумных» в терминах [10]) управленческих решений. Предлагается несколько примеров расчета результативности СМИБ, прошедших практическую апробацию.

2. Необходимые термины и определения. Для решения поставленной проблемы рассмотрим несколько необходимых терминов из [1] и [11]:

1. *Событие информационной безопасности* (*information security event*): идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. Отметим, что это определение точно совпадает по п. 3.5 в [1]и по п. 3.2 [11].

2. *Инцидент информационной безопасности* (*information security incide*nt): Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ (п. 3.3. по [11]). Но в стандарте [1] представлено иное определение: «*Инцидент информационной безопасности* (*information security incident*): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность» (п. 3.6. по [1]).

Обратим внимание, что «целевой» стандарт по сертификации СМИБ [1] трактует термин «инцидент ИБ» иначе, чем стандарт по управлению инцидентами ИБ [11]. Прежде всего, стандарт [11] устанавливает четкую логическую последовательность – инцидент ИБ является следствием события (событий) ИБ. В тоже время определение по [11] объективно более емкое – дает четкую «привязку» на бизнес-активы и угрозы ИБ, что подразумевает некоторый «операционный» анализ, выполняемой в организации, исходя из внутренних потребностей, технических возможностей и целей ИБ.

Следующие термины важны для ясного и однозначного понимания «предмета измерения». Расчет результативности СМИБ [1] выполняется в точном соответствии в терминах по ГОСТ Р ИСО серии 9000, в котором приведены следующие два термина:

3. *Результативность* (*effectiveness*): степень реализации запланированной деятельности и достижения запланированных результатов (п. 3.2.14)

4. *Эффективность* (*efficiency*): Связь между достигнутым результатом и использованными ресурсами (п. 3.2.15)

В методическом плане представляется рациональным говорить именно об оценке результативности СМИБ, т.к. для оценки эффективности нужно оперировать дополнительно затраченными ресурсами: финансовыми параметрами деятельности организации и, детально, динамикой их изменения (бюджет службы ИБ, штатная численность, стоимость технических средств (ТС), внешние услуги и пр.) [12 – 15]. Дополнительно принимается во внимание, что выбор мер (средств) обеспечения ИБ (“controls”) для ИС является важной задачей, которая может иметь значительные последствия в отношении бизнес-операций и защищаемых активов организации, а также вовлеченного персонала, что также вносит существенные бюджетные решения и процесс капиталовложений [2, 16 – 17].

3. Определение сущностей для расчета результативности. Для практической реализации выбранных ключевых сущностей и достоверной оценки результативности СМИБ потребуются выполнить определенные предположения. Появляется роль «оператора», который в режиме, близком к режиму реального времени (РРВ), анализирует совокупность событий (их может быть несколько тысяч в достаточно краткий период) и принимает решение о фиксации события ИБ и/или инцидента ИБ – в случае если нанесен ущерб. В расчете результативности СМИБ предлагается применять три ключевые сущности: Событие, Событие ИБ и Инцидент ИБ.

1. *Событие* – любое изменение установленного состояния контролируемых объектов. (event, alert, «сработка» ТС и/или СЗИ). События фиксируются в журналах (проход сотрудника через КПП), в log-файлах (межсетевые экраны), в архивах (системы видеонаблюдения) и пр. Важно, что событие всегда «идентифицировано», т.е. является материальным фактом, может быть извлечено, проанализировано «оператором», передано на дальнейшую обработку, протестировано на стенде и пр. Важно также, что событие само по себе не приводит к угрозам ИБ, тем более – к ущербу ИБ (бизнесу). Предполагается, что число событий может быть велико и достигать нескольких тысяч в день, это обстоятельство накладывает определенные ограничения на «глубину» архива и временной лимит для анализа (обработки) «сырых» событий со стороны оператора. *Должно выполняться*: Кол-во событий > 0.

2. *Событие ИБ* – результат анализа множества «сырых» событий со стороны оператора. Анализ событий ИБ выполняется на основании определенных критериев (например, количество ошибок при вводе пароля, количество просроченных сертификатов ЭЦП и пр.). Важно, что в качестве событий ИБ могут выступать записи аудитов – внутренних и внешних, которые также являются фиксированными событиями (см. выше). Предполагается, что по факту события ИБ может быть предпринято расследование (при эскалации как инцидент ИБ). Предполагается, что число событий ИБ может достигать сотни в год. *Должно выполняться*: Кол-во событий > Кол-во событий ИБ.

3. *Инцидент ИБ* – в нотации ГОСТ 18044 [11] это следствие проявления событий ИБ, что возможно приведет к компрометации бизнеса или угрозе ИБ. Важно, что инцидент является именно следствием события ИБ, на основании решения «оператора» по итогам анализа события ИБ. Для каждого идентифицированного инцидента ИБ принимается решение о вероятности реализации угроз и возникновения ущерба (например, угроза финансовых потерь при передаче носителя с сертификатом ЭЦП неуполномоченному лицу). По инциденту ИБ всегда проводится расследование с отражением факта преодоления (попытки) существующих мер и средств обеспечения ИБ ("*controls*"), оценке конкретного ущерба ИБ. Предполагается, что число инцидентов ИБ может достигать десятков в год. *Должно выполняться*: Кол-во событий ИБ > Кол-во инцидентов ИБ.

4. Установленные дополнительные ограничения для расчета. Практическая реализация выбранных сущностей требует

фиксации дополнительных ограничений по выполненным ранее предположениям:

1. *Область сертификации СМИБ (“scope”)* – если выбрано на определенный период только несколько процессов (например, обеспечение ИБ для работы в сети интернет), то ошибки ввода паролей в АСУТП не принимаются при расчетах ни количества событий ИБ, ни инцидентов ИБ.

2. *Временной интервал* – необходимо выполнять сравнение между состоянием «*до СМИБ*», т.е. когда ТС были внедрены, но сама система СМИБ формально не вводилась в действие, персонал не проходил должного обучения и определенные дополнительные нормативные документы (регламенты) не разрабатывались и текущим состоянием, отсчитываемым, например, по годам.

3. *Техническая возможность* – необходимо обеспечить техническую возможность по обработке значительного количества событий в режиме, близком к режиму реального времени (РРВ) по структурным подразделениям и «селекции» событий ИБ, которые попадают в *scope* текущей конфигурации СМИБ.

4. *Оператор* – необходимо обеспечить наличие «оператора», доступность, компетентность и оснащенность которого позволяет принимать решения в фиксированном временном интервале о назначении события ИБ и/или инцидента ИБ в силу достоверной и объективной информации по множеству входных событий.

5. *Норма допустимой результативности* – необходимо обеспечить учет «порогового» допустимого значения, которое является ориентиром для расчета текущего уровня результативности СМИБ (в текущей конфигурации ***scope***). В расчете «порогового» допустимого значения участвует плановый (задаваемый ЛПР) показатель повышения результативности СМИБ, например, 10%.

6. *Зрелость СМИБ* – необходимо принять во внимание, что для СМИБ, находящихся на разных уровнях зрелости, представляется целесообразным применять разные формулы определения результативности. В частности, на первом этапе «приработки» СМИБ могут применяться простые формулы, с увеличением опыта и технического оснащения (“***controls***”) могут применяться полиномы с системой весовых коэффициентов, расчет которых представляют отдельную задачу.

5. Формулы расчета результативности СМИБ. С учетом сказанного выше для СМИБ рекомендуются к применению следующие формулы, учитывающие, например, раздельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая

оснащенность «оператора», о чем указывалось выше. В частности, реализованный в СМИБ комплекс ТС должен позволять «селектировать» из многих тысяч событий в режиме, близком к РРВ, события, относящиеся к сотрудникам одной службы, даже если они находятся в разных подсетях (VLAN). Соответственно, результативность СМИБ рассчитывается следующим образом:

Расчет результативности событий ИБ:

$$\text{К с} = \left(\mathbf{1} - \left(\frac{\text{С тек.}}{\text{С } max}\right)\right) * \mathbf{100}\%, \quad (1)$$

где:

Кс – коэффициент результативности идентификации событий ИБ;

С***тек*** – идентифицированное количество событий ИБ в текущей конфигурации ***scope***;

С***max*** – максимально возможное количество событий ИБ за предыдущий период.

Расчет результативности инцидентов ИБ:

$$\text{К и} = \left(\mathbf{1} - \left(\frac{\text{И тек.}}{\text{И } max}\right)\right) * \mathbf{100}\%, \quad (2)$$

где:

Ки – коэффициент результативности идентификации инцидентов ИБ;

И ***тек*** – идентифицированное количество инцидентов ИБ в текущей конфигурации scope;

И ***max*** – максимально возможное количество инцидентов ИБ за предыдущий период.

С учетом положений (1) и (2) общий показатель результативности СМИБ рассчитывается:

$$\text{К смиб} = (\text{К с} * \boldsymbol{\alpha} + \text{К и} * \boldsymbol{\beta}), \quad (3)$$

где:

К смиб – общий показатель результативности СМИБ

Кс – коэффициент результативности идентификации событий ИБ;

Ки – коэффициент результативности идентификации инцидентов ИБ;

α – весовой коэффициент определения важности Кс;

β – весовой коэффициент определения важности Ки.

Формула (3) обладает рядом особенностей:

1. При С***тек*** = 0 и И***тек*** = 0 мы получаем абсолютный 100% уровень ИБ, несмотря на ведущийся «лог» многочисленных «сырых» событий. Если «оператор» не выделил события ИБ (нет «видимых»

нарушений ИБ), не определил инциденты ИБ (нет ущерба ИБ или компрометации бизнес-процессов).

2. Весовые коэффициенты α и β нормируются к единице (α + β= 1) и определяют значимость для конкретного объекта (процесса СМИБ) значимость событий и инцидентов ИБ. В простейшем случае α = β = 0,5.

6. Примеры кейсов для расчета результативности СМИБ. Рассмотрим несколько практических примеров расчета результативности СМИБ по формуле (3) для случая зрелой СМИБ.

Кейс 1.

Для С***тек*** = 54, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 21, α = β = 0,5 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{54}{60}\right) * 100\%\right) * 0{,}5 + \left(1 - \left(\frac{18}{21}\right) * 100\%\right) * 0{,}5\right) = 12{,}14\%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель достигнута.

Кейс 2.

Для С***тек*** = 70, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 23, α = β = 0,5 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{70}{60}\right) * 100\%\right) * 0{,}5 + \left(1 - \left(\frac{18}{23}\right) * 100\%\right) * 0{,}5\right) = -8{,}33 + 10{,}86 = 2{,}53\%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель не достигнута.

Кейс 3.

Для С***тек*** = 70, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 23, α = 0,3 β = 0,7 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{70}{60}\right) * 100\%\right) * 0{,}3 + \left(1 - \left(\frac{18}{23}\right) * 100\%\right) * 0{,}7\right) == -5 + 15{,}21 = 10{,}21\ \%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель достигнута.

7. Дополнительные метрики ИБ, применяемые для оценки результативности СМИБ. С целью снижения ущерба и потери ценных для бизнеса активов, для службы ИБ предлагаются метрики, показывающие степень достижения возможного максимума (плана продаж, выполнения в срок проектов и пр.) [12, 15–17]. Соответственно, могут быть предложены различные типы метрик:

— простые метрики (например, количество выявленных инцидентов ИБ, предотвращенных утечек);

— сложные метрики (например, отношение стоимости мер защиты к стоимости ИТ активов);

— комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в ИС, определенных как критичные для бизнеса).

В качестве практических метрик ИБ рекомендуются к применению:

— Кс = (1 – С тек * 100% / С макс) – для оценки динамики событий ИБ;

— Кр = (1 – Кс (повторных) * 100% / Кс) – для оценки динамики повторных событий ИБ (рецидив);

— Кд = (С макс – С тек) / (К макс – К тек) – для оценки динамики приращений событий ИБ и инцидентов ИБ.

8. Выводы:

1. Для оценки результативности СМИБ (вне зависимости от целей, типов и частоты аудитов), необходимо обеспечить управление достоверными и удобными для анализа численными метриками ИБ. Представляется важным, что оценки результативности СМИБ явным образом влияют на изменение статуса службы ИБ, и соответствующего технического оснащения (бюджета). В то же время предоставление «слабых» оценок ИБ может быть расценено как несоответствие понимания роли службы ИБ в обеспечении успешного достижения бизнес-целей организации.

2. При создании СМИБ, соответствующих множеству требований (отраслевой сертификации, национальным стандартам ГОСТ Р, международным стандартам ISO) в общем случае, необходимо учитывать и уникальные отраслевые особенности – например, с помощью весовых коэффициентов. Но в этом случае, как было показано в практических примерах (кейсах), существует сложность выделения по значимости какой-либо одной сущности, группы активов или набора технических средств.

3. При прогнозировании и обеспечения постоянного повышения результативности СМИБ необходимо формировать сопоставимые метрики ИБ, которые позволят оценить сделанные предварительно предположения и допущения и сформировать обоснованные цели в области СМИБ, направленные на обеспечение стабильного развития бизнеса организации.

Литература

1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // М.: ФАТРиМ России. 2008.
2. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности // М.: ФАТРиМ России. 2011.
3. ГОСТ Р ИСО 19011-2011 Руководящие указания по проведению аудитов систем менеджмента // М.: ФАТРиМ России. 2013.
4. СТО Газпром 4.2-1-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Основные термины и определения // М.: ОАО «Газпром». 2009.
5. СТО Газпром 4.2-2-002-2009 Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами // М.: ОАО «Газпром». 2009.
6. СТО Газпром 4.2-3-002-2009 Требования по технической защите информации при использовании информационных технологий // М.: ОАО «Газпром». 2009.
7. СТО Газпром 4.2-3-003-2009 Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков // М.: ОАО «Газпром». 2009.
8. СТО Газпром 4.2-3-004-2009 Классификация объектов защиты // М.: ОАО «Газпром». 2009.
9. СТО Газпром 4.2-3-005-2013 Управление инцидентами информационной безопасности // М.: ОАО «Газпром». 2013.
10. *Ногин В.Д.* Принятие решений при многих критериях // Государственный Университет – Высшая школа экономики. Санкт-Петербург. 2007. 103 с.
11. ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности // М.: ФАТРиМ России, 2008.
12. *Карпенко М.С.* Учет факторов риска и неопределенности при реализации энергосберегающих проектов // Энергобезопасность и Энергосбережение. 2014. Вып. 6. С. 13–16.
13. *Лившиц И.И.* Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и Связь. 2013. Вып. 6. С. 62–67
14. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
15. *Лившиц И.И.* Актуальность применения метрик информационной безопасности для оценки результативности проектов систем менеджмента информационной безопасности // Менеджмент качества. 2015. Вып. 1. С. 74–81
16. NIST.SP.800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. URL: http://dx.doi.org/10.6028/
17. *Брукс П.* Метрики для управления ИТ-услугами // Альпина Бизнес Букс. 2007. 270 с.

References

1. GOST R ISO/IEC 27001:2005. [Information technology. Security techniques. Information security management systems. Requirements].M.: FATRiM Rossii. 2008. (In Russ.).
2. GOST R ISO/IEC 27005:2010. [Information technology. Security techniques. Information technology. Security techniques. Information security risk management]. M.: FATRiM Rossii. 2011. (In Russ.).
3. GOST R ISO 19011:2011. [Guidelines for auditing management systems]. M.: FATRiM Rossii. 2013. (In Russ.).

4. STO Gazprom 4.2-1-001-2009. [IT-Security Providing System. Terms and Definition]. M.: OAO Gazprom. 2009. (In Russ.).
5. STO Gasprom 4.2-2-002-2009. [IT-Security Providing System. Requirements for automated process control system]. M.: OAO Gazprom. 2009. (In Russ.).
6. STO Gasprom 4.2-3-002-2009. [IT-Security Providing System. Requirements for technical protection of information when using information technology]. M.: OAO Gazprom, 2009. (In Russ.).
7. STO Gasprom 4.2-3-003-2009. [IT-Security Providing System. Analyses and assessment of Risk]. M.: OAO Gazprom. 2009. (In Russ.).
8. STO Gasprom 4.2-3-004-2009. [IT-Security Providing System. Object of protection classification]. M.: OAO Gazprom. 2009. (In Russ.).
9. STO Gasprom 4.2-3-005-2013. [IT-Security Providing System. IT-Security Incident Management]. M.: OAO Gazprom. 2009. (In Russ.).
10. Nogin V.D. *Prinyatie resheniy pri mnogih kriteriyah* [Decision-making in many criteria]. St. University, St. Petersburg, 2007. 103 p. (In Russ.).
11. GOST R ISO/IEC 18044-2007. [Information technology. Security techniques. Information security incident management]. M.: FATRiM Rossii, 2008. (In Russ.).
12. Karpenko M. [Managing the risks and uncertainties in the implementation of energy saving projects]. *Jenergobezopasnost' i Jenergosberezhenie – Energy Security and Energy Saving*. 2014. vol. 6. pp. 13–16 (In Russ.).
13. Livshitz I.I. [Joint problem solving information security audit and ensure the availability of information systems based on the requirements of international standards BSI / ISO]. *Informatisatia i Svyaz' – Informatization and Communication.* 2013. vol. 6. pp 48–51 (In Russ.).
14. Livshitz I.I. [Practical purpose methods for ISMS evaluation]. *Menedzhment kachestva – Quality Management*. 2013. vol. 1. pp. 22–34 (In Russ.)..
15. Livshitz I.I [Actuality of IT-security metrics appliance for ISMS evaluation]. *Menedzhment kachestva – Quality Management.* 2015. vol. 1. pp. 74–81 (In Russ.).
16. NIST.SP.800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Available at: http://dx.doi.org/10.6028.
17. Bruks P. *Metriki dlja upravlenija IT-uslugami* [Metrics for IT-service management]. Alpina Business Books. 2007. 270 p. (In Russ.).

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.

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.

Полещук Александр Владимирович — к-т техн. наук, эксперт по информационной безопасности, ООО «Академия Информационных Систем». Область научных интересов: системный анализ, защита информации, управление событиями и инцидентами ИБ. Число научных публикаций — 50. sailor1981@rambler.ru; ул. Плеханова, 4а, Москва, 111141; р.т.: +7 (495) 817-08-70.

Poleshuk Alexander Vladimirovich — Ph.D., IT-Security expert, JSC "IT-System Academia". Research interests: system analyses, IT-security, IT-security incident and events management. The number of publications — 50. sailor1981@rambler.ru; 4a, Plehanova, Moscow, 111141, Russia; office phone: +7 (495) 817-08-70.

РЕФЕРАТ

Лившиц И.И., Полещук А.В. **Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром.**

В данной публикации рассмотрена проблема оценки результативности СМИБ в соответствии с требованиями стандартов ИСО серии 27001. Более сложной проблемой является проблема обеспечение постоянного улучшения результативности СМИБ, созданной с учетом дополнительных отраслевых стандартов (например, СОИБ Газпром). Решение поставленной выше проблемы может быть затруднено объективными различиями в требованиях СОИБ, которые могут усложнить успешное внедрение СМИБ (например, различия в понятиях «актив» и «объект защиты»). В равной мере это относится и к требованиям по менеджменту рисков, а также правилам проведения аудитов в соответствии со стандартом ИСО серии 19011.

Стандарт ИСО 27001 трактует термин «инцидент ИБ» иначе, чем стандарт ИСО 18044, отмечено, что стандарт по управлению инцидентами устанавливает четкую логическую последовательность – инцидент ИБ является следствием события (событий) ИБ. Это определение по ИСО 18044 объективно более емкое – дает четкую «привязку» на бизнес-активы и угрозы ИБ, что подразумевает некоторый «операционный» анализ, выполняемой в организации, исходя из внутренних потребностей и целей ИБ.

Для СМИБ рекомендуются к применению следующие формулы, учитывающие, например, раздельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая оснащенность «оператора». В частности, реализованный в СМИБ комплекс технических средств должен позволять «селектировать» из многих тысяч событий в режиме, близком к реальному времени, события, относящиеся к сотрудникам одной службы, даже если они находятся в разных подсетях (VLAN). Соответственно, результативность СМИБ рассчитывается с учетом уникальных отраслевых особенностей – например, с помощью весовых коэффициентов. Представляется важным, что оценки результативности СМИБ явным образом влияют на изменение статуса службы ИБ, и соответствующего технического оснащения (бюджета). В то же время предоставление «слабых» оценок ИБ может быть расценено как несоответствие понимания роли службы ИБ в обеспечении успешного достижения бизнес-целей организации. Данные результаты могут найти применение при создании моделей и методов обеспечения аудитов СМИБ и мониторинга состояния объектов, находящегося под воздействием угроз нарушения ИБ, а также при создании моделей и методов оценки защищенности информации и ИБ объектов СМИБ и/или СОИБ Газпром.

SUMMARY

Livshits I.I., Poleshuk A.V. **Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.**

This issue covers the problem of assessing ISMS effectiveness in accordance with the requirements of ISO 27001 series and more complex problems – concerning ensuring the continuous improvement for ISMS effectiveness, created with the additional industry standards (eg, STO ISPS Gazprom). The solution of the above problems can be complicated by objective differences in the requirements ISPS that can complicate the successful ISMS implementation (eg, differences in terms of "asset" and "object of protection"). This equally applies to the requirements for risk management, as well as the rules of the audits in accordance with ISO 19011 series.

ISO 27001 interprets the term "security incidents" other than ISO 18044, it is noted that the standard incident management establishes a clear logical sequence – the IT-security incident is a consequence of the IT-Security event (s). This definition is in accordance with ISO 18044 objectively more capacious - gives a clear "links" on the business assets and threats to IT-Security, which implies a certain "operational" analysis performed by the organization on the basis of domestic needs and IT-Security objectives.

For ISMS it recommended to use the following formulas, taking into account, for example, separate IT-Security incidents and IT-Security events. In this embodiment, a special role is played by the technical equipment of "operator". In particular, implemented in ISMS set of technical tools should allow to "select" more than thousands of events per short period related to a single service employees, even if they are on different subnets (VLAN). Accordingly, the ISMS effectiveness is calculated with taking into account the unique features of the sector - for example, using weighting factors. It is important that the assessment of ISMS effectiveness explicitly affect the change in the status of IT-Security department, and the appropriate technical equipment (budget). At the same time providing the "weak" estimates of IT-Security can be regarded as inconsistent with the understanding of the role of IT-Security department to ensure the successful achievement of the business objectives of the organization. These results can be used to create models and methods to ensure the ISMS audits and monitoring of objects under the influence of threats to IT-Security violations, as well as the creation of models and methods of estimation of IT-Security facilities ISMS and / or ISPS Gazprom.