**УДК** 004.94

И.И. Лившиц

# ПОДХОДЫ К СИНТЕЗУ МОДЕЛИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ СТАНДАРТА ISO/IEC 27001:2005

*Лившиц И.И.* **Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005**

**Аннотация.** Анализ публикаций за последние несколько лет по проблеме проектирования, внедрения и сопровождения систем защиты персональных данных (ПДн) позволяет отметить стабильно высокий интерес к этому актуальному и критичному аспекту обеспечения ИБ. Определенно предлагаемые различными специалистами подходы к синтезу моделей на базе как международных, так и отечественных стандартов свидетельствует о глубокой проработке всех требований по защите ПДн, но в тоже время ставят новые вопросы, эффективное решение которых экспертам еще только предстоит синтезировать и проверить на практике.

В предлагаемой работе предложены некоторые подходы для создания модели оценки защищенности ПДн в соответствии с требованиями стандарта ISO/IEC 27001:2005. Учитывая относительную новизну данного стандарта в практическом применении к исследуемой проблеме, предлагаемые подходы могут оказаться полезными при планировании систем защиты ПДн, оценке защищенности уже созданных ИСПДн, а также, в частности, для решения практических задач — аудитов ИБ в организациях.

**Ключевые слова:** активы, информационная безопасность (ИБ), персональные данные (ПДн), система менеджмента информационной безопасности (СМИБ), средства защиты информации (СЗИ), несанкционированный доступ (НСД), аудит.

*Livshitz I.I.* **The approaches for model's synthesis of private data security assessment in accordance with ISO/IEC 27001:2005 standards requirements**.

**Abstract.** The analysis of recent publications concerning an approaches to design, implementation and maintenance of the systems for personal data (PD) protection enables to note consistently high interest in this critical problem in the aspect of ensuring information security. Sure, the proposed models based on both International and Russian standards indicate deep-in-side knowledge of all aspects of protection PD, but at the same time present new questions, an effective solution of which has yet to be synthesized and tested in practice.

The present article provides some approaches for creating models of PD security assessment in accordance with the requirements of standard GOST R ISO/IEC 27001:2005. Taking into account the relative newness of this standard as applied to the research problem, the proposed approaches can be useful in planning security systems PD, security assessment of designed IT-Security with PD and, in particular, in solving of practical problems - IT-Security audits in organizations.

**Keywords:** assets, IT-security, risk-management, private data (PDn), assessment, standard, IT-security management system (ISMS), security controls, non-authorized access, audit, requirements.

**1. Введение.** В последнее время в Российской Федерации (РФ) обеспечение информационной безопасности (ИБ) ценных информационных активов находится в фокусе внимания как одна из ключевых проблем для обеспечения стабильности как организаций, так и на уровне государства. Техническое обеспечение для решения данной проблемы постоянно совершенствуется, появляются новые средства защиты информации (СЗИ), препятствующие или существенно затрудняющие попытки несанкционированного доступа (НСД). В области законодательного регулирования в РФ принят ряд нормативных правовых актов (НПА), прежде всего ряд Федеральных законов (ФЗ): ФЗ-8453-1 «О государственной тайне», ФЗ-149 «Об информации, информационных технологиях и о защите информации», ФЗ-98 «О коммерческой тайне», ФЗ-152 «О персональных данных» [1],[2]; Постановления Правительства, «Руководящие документы» ФСТЭК [3], а также комплекс СТО БР ИББС [4], [5], [6].

Необходимо отметить, что в РФ активно вводятся в оборот международные стандарты (МС), призванные восполнить пробел в создании современных систем менеджмента информационной безопасности (СМИБ), отвечающим требованиям как бизнеса (прежде всего эффективности), так и законодательным требованиям различных регуляторов (т.н. «compliance»). Среди наиболее известных МС необходимо отметить стандарты ИСО/МЭК серии 27000 [7], [8], [9]; 20000; стандарты BSI серии 25999; американские стандарты NIST, стандарты Австралии и Новой Зеландии AS/NS 4360 и пр.

Одним из наиболее критичных видов информации, защита которых затронула практически все слои современного общества, являются персональные данные (ПДн). О фактах крупнейших утечек ПДн как в РФ, так и за границей известно достаточно; причем ущерб, в отличие от хищения материальных средств, больше имиджевый – несколько атак подряд на серверы Sony привели к утечке личной информации более 1 млн. пользователей (по данным Reuters). В частности, в июне 2011 очередное нападение было осуществлено хакерской группой LulzSec. Взломщики опубликовали имена, даты рождения, электронные адреса, номера телефонов и пароли нескольких тысяч участников конкурсов, которыми владела Sony.

В стандарте [9] предложена система деления активов (п. 2.3) по 6 категориям (важнейшими из которых признаются информационные). При этом необходимо отметить, что и в «узком» аспекте безопасности ПДн и, если рассматривать проблему шире – для решения проблемы оценки эффективности ИБ, необходимо оценивать всю совокупность

активов в организации: и программные средства, и сетевые коммуникации, и аппаратное обеспечение, иными словами, все компоненты ИСПДн.

Для специалистов – инженеров, юристов, сотрудников отделов персонала и служб безопасности проблема обеспечения эффективности защиты ПДн недостаточно отработана в силу сложностей оценки защищенности технических средств (информационных систем, ИС). Как следует из ФЗ-152, проблема защиты ПДн актуальна прежде всего в ИСПДн, которые могут «в базовом варианте» разработки и поставки не содержать встроенных систем СЗИ НСД. Особенно это замечание справедливо для АС, созданных достаточно давно (например, ЗАГС или поликлинический медицинской АС) и категорированных как ИСПДн только в связи с требованиями ФЗ-152.

Необходимо отметить, что и при наличии достаточного количества регулирующих технических документов (ГОСТ Р 51583-2000) наличие требований по ИБ в ГОСТ серии 34 (например 34.601, 34.201,) и др. обработка ПДн в ряде ИСПДн проходит без должного внимания к проблемам ИБ даже у крупнейших операторов (пример – в сахалинском филиале ОАО «Дальсвязь» выложили на публичный FTP-сервер файлы с исчерпывающими служебными и личными данными как минимум 11 тыс. существующих или бывших клиентов). Для формирования эффективной системы анализа защищенности ПДн необходимо применять комплексный подход, включающий ряд взаимоувязанных мероприятий, одним из важнейших является формирование системы критериев и разработка моделей оценки защищенности ПДн.

ISO/IEC 27001:2005 предлагает концепцию ИБ, построенную на «триаде безопасности» - обеспечении конфиденциальности, целостности и доступности. Важно отметить, что в стандарте предлагается комплексный подход, учитывающий различные аспекты ИБ (физический, организационно-административный, технический, юридический и пр.), и стандарт содержит универсальные принципы, которые в равной мере позволяют предоставить независимые оценки СМИБ. В области применения [7] отмечено, что *«настоящий международный стандарт определяет требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию документированной СМИБ в контексте общих бизнес-рисков организации».*

Стандарт [8] предлагает процесс менеджмента рисков ИБ, который включает несколько последовательных шагов (идентификация, оценка, обработка и пр.) и две «критические точки принятия решения»: обрабатывать ли конкретный риск и считается ли определенный

риск приемлемым. В аспекте анализа защищенности ПДн неизбежно потребуются экспертные оценки, т.к. для принятия решения (например, как было показано выше) необходимо постоянно оценивать новые уязвимости, проводить детальный анализ защищенности и оценивать изменения перечня СЗИ НСД в фокусе постоянно меняющихся угроз.

Анализ НПА в области ИБ в РФ показывает, что до настоящего времени не уделялось должного внимания вопросам формирования требований и критериев оценки защищённости ПДн. Отдельные требования присутствуют, очевидно, и в МС, BS, РД ФСТЭК и ФСБ, но конкретных методик оценки (качественных или количественных) пока не предложено. При оценке защищенности ПДн известны трудности, связанные с проблемами формализации требований (критериев) предметной области и использованием статистической информаций. Это обусловлено неоднородностью выборки статистической информации, возникающей из-за разнообразия ИТ-технологий, ПО и СЗИ, используемых при защите ПДн [10], [11]. В связи с этим в большинстве случае для оценки защищенности ПДн применяются экспертные оценки характеристик ИБ. Проведенный анализ тенденций в оценке защищенности ПДн и особенностей практической интерпретации обработки результатов такой оценки позволил сделать вывод, что для повышения объективности и корректности оценки защищенности ПДн необходимо использовать методы и модели многокритериальной оценки, позволяющие обрабатывать трудно формализуемые данные.

Большинство методов оценки защищенности ИБ, применимых и к ПДн, используют классификационный подход, который основан на широком использовании экспертных оценок. Известно общее свойство оценок с участием экспертов - наличие разноплановой информации, трудно формализуемой в рамках традиционных математических алгоритмов. Основной причиной трудностей в формализации, необходимой для оценки ПДн, является факт, что эксперты при оценивании реальных уникальных объектов используют многолетний опыт и отработанные на практике методики и подходы [12].

Проведенные исследования и практика аудитов ИБ на соответствие требованиям ISO/IEC 27001:2005 показали, что синтез модели оценки защищенности ПДн можно условно разделить на 2 этапа:

1. Получение исходных данных для оценки, включая анализ документации по разработке, интеграции, эксплуатации и мониторингу текущей (мгновенной) защищенности ПДн;

2. Оценивание защищенности ПДн, включая аттестацию ИСПДн (сертификацию СМИБ) в соответствии с установленными критериями.

***Первый этап*** – сбор информации и идентификация проблемы принятия решения. На этом этапе определяются альтернативы, которые следует изучить в деталях, насколько это представляется целесообразным и допустимым. Далее происходит выбор одного из вариантов решений из множества альтернатив, подготовленных (оцененных экспертами) ранее.

***Второй этап*** – реализация выбранной альтернативы и обобщение опыта, полученного в процессе решения проблемы. Дополнительно на этом этапе предполагается построение экономической модели оценки эффективности представленного решения.

Для решения проблемы сравнения и оценки альтернатив в указанных ситуациях наиболее целесообразен метод сравнения альтернатив относительно стандартов [13], [14]. «Классический» метод парного сравнения альтернатив не всегда может быть эффективно применен в практических ситуациях в силу основных причин:

- экспертам может быть предложено для анализа более 7 альтернатив, что существенно усложняет построение согласованных матриц парных сравнений (обратим внимание, что при увеличении альтернатив свыше 15, метод парных сравнений считается неприменимым);
- альтернативы могут поступать эксперту для сравнения не одновременно, а через определенные промежутки времени. Поэтому невозможно попарно сравнивать объекты.

Для оценки защищенности ПДн в качестве «предметной нормативной базы» принимается объединенная концептуальная модель, включающая требования Приложения «А» в ISO/IEC 27001:2005 (перечень «контролей», сгруппированных по 11 разделам А.5 – А.11), усиленная средствами защиты ПДн и комплексом административных мероприятий в соответствии с требованиями руководящего документа ФСТЭК (см. Таблицу № 1)

Таблица 1. **Пример выбора «контролей» для оценки защищенности ПДн**

| Аспект «триады» ИБ в ИС-ПДн | Пункт ISO/IEC 27001:2005 | Требование |
|---|---|---|
| **Целостность** | **A.10.1.3** | «Обязанности и области ответственности должны быть разделены с целью снижения количества возможностей неразрешенного или непреднамеренного изменения или неправильного использования активов организации». |
| | **A.9.2.4** | Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности. |

| | | |
|---|---|---|
| **Конфиденциальность** | **A.6.1.5** | Требования по конфиденциальности или соглашения о неразглашении, отражающие потребности организации в защите информации, должны быть определены и регулярно пересматриваться. |
| | **A.7.1.3** | Должны быть определены, документированы и внедрены правила для приемлемого использования информации и активов, связанных со средствами, обрабатывающими информацию. |
| **Доступность** | **A.9.2** | «Предотвратить гибель, ущерб, кражу или компрометацию активов и заминку в работе организации» |
| | **A.14.1.3** | Должны быть разработаны и внедрены планы для поддержки или восстановления работы и гарантии доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критичных бизнес-процессов. |

Стандарт устанавливает уровень качества объекта относительно критерия качества. Каждый стандарт отождествляется, как правило, с некоторым существующим на практике «эталоном». По известной [13] модели иерархии стандарты присваиваются элементам, имеющим непосредственную связь с альтернативами (см. рис.1). Число стандартов по каждому такому элементу может быть различно и определяется экспертом

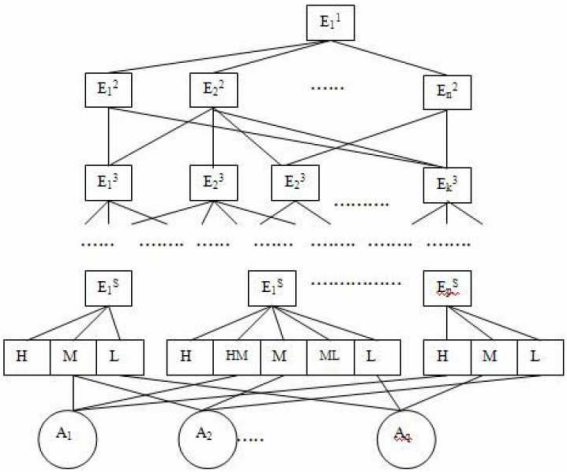


Рис. 1. Пример построения модели иерархической структуры с учетом стандартов.

По каждому стандарту экспертом (независимыми группами экспертов) устанавливается относительная степень предпочтения, которая указывает значимость стандарта для эксперта. Численное значение каждого стандарта определяется их попарным сравнением по шкале отношений.

Например, для критерия «***Целостность***» может быть выбрано следующее множество стандартов: СТО БР ИББС, ГОСТ Р ИСО/МЭК и РД ФСТЭК, каждый из которых характеризует экспертное мнение относительно «высокого» (**В**), «среднего» (**С**) и «низкого» (**Н**) уровня по отношению к рассматриваемому критерию. Строго говоря, экспертам могут быть предложены несколько шкал, допускающих более точные, при необходимости, градации, в отношении определенного выбранного критерия, например: (**ВВ**), (**ВС**), (**СН**),…

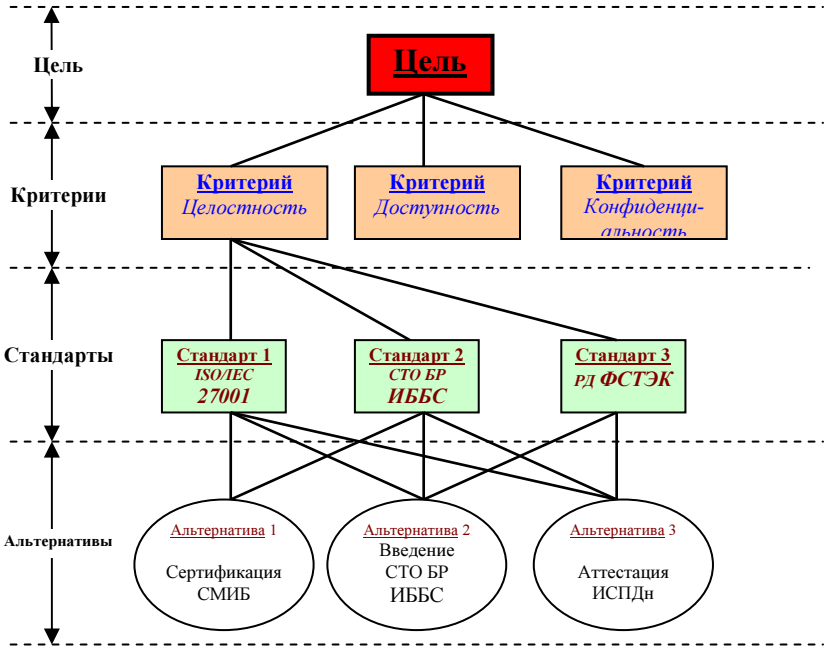


Рис. 2. Пример построения модели иерархической структуры с учетом 3-х стандартов.

Для выбранного множества, например, из 3-х стандартов таблица предпочтений будет иметь вид матрицы размерности 3 (Таблица № 2):

Таблица 2. **Пример построения матрицы предпочтения стандартов**

| | **B** | **C** | **H** |
|---|---|---|---|
| **B** | **1** | **5** | **7** |
| **C** | **1/5** | **1** | **2** |
| **H** | **1/7** | **1/2** | **1** |

Для указанного примера главный собственный вектор

$$\mathbf{W} = \{0.729;0,179;0,09\}^{\mathbf{T}}$$

Оценим ***Индекс согласованности*** (ИС) и ***Отношение однородности***, соответственно:

**ИС = 0,032**
**ОС = 0,056**

Согласованность служит, как известно, индексом «качества» представленных экспертных мнений, при **ОС** < 0,10 экспертные данные считаются приемлемыми (однородными); при превышении указанного порога данные необходимо уточнить.

Комментарий: Для выбранного критерия «**Целостность**» группа экспертов применительно к ИСПДн «Объект «Альфа» полагает, что стандарт «**B**» (ISO/IEC 27001: 2005) определенно важнее по сравнению с комплексом безопасности «**C**» (СТО БР ИББС) и значительно важнее относительно руководящих документов по защите ПДн «**H**» (РД ФСТЭК).

Исходя из общей структуры критериев и особенностей формирования альтернатив для построения метода оценки защищенности ПДн предлагаются следующие принципы создания модели оценки защищенности ПДн.

*Принцип 1* – приоритет множества критериев перед видом (выбором) последующего метода оценки;

*Принцип 2* – альтернативы определяются (базируются) на экспертных оценках, полученных от независимых групп специалистов.

*Принцип 3* – соответствие количества градаций оцениваемых величин (при формировании списка критериев, перечня альтернатив, матрицы предпочтения стандартов) «доверительному» уровню оценки групп экспертов.

В соответствии с предложенными принципами модель многоуровневой оценки защищенности ПДн состоит из следующих последовательных процедур:

1. Процедура сбора информации (подготовки данных от независимых групп экспертов);
2. Процедура формирование перечня критериев и построение альтернатив;
3. Процедура выборов альтернативы;
4. Процедура оценки и анализ результата.

В таблице 3 предложена методика выполнения оценки защищенности ПДн.

Таблица 3. **Методика оценки защищенности ПДн**

| № | Фаза | Детализация задач |
|---|---|---|
| 1 | **Сбор информации** | 1.Определение цели<br>2.Формирование независимых групп экспертов<br>3.Определение перечня критериев<br>4.Определение комитета, принимающего решение |
| 2 | **Построение альтернатив** | 1.Уточнение перечня критериев<br>2.Формирование матрицы для построения альтернатив<br>3.Построение альтернатив |
| 3 | **Выбор альтернатив** | 1.Построение матрицы предпочтения стандартов<br>2.Построение шкал оценки (основной и дополнительной)<br>3.Выбор альтернативы1-й независимой группы экспертов<br>4.Повторный выбор альтернативы на основе данных 2-й независимой группы экспертов |
| 4 | **Оценка результатов** | 1.Анализ результатов выбора альтернативы<br>2.Анализ возможности конструирования альтернатив<br>3.Подготовка отчета комитету, принимающему решение. |

**Заключение.** При обеспечении комплексной безопасности современной организации важное практическое значение приобретает проблема ***численной оценки уровня защищенности***. В конкретном аспекте ИБ – защищенность ПДн является необходимой как в силу

законодательного требования (объективно – как в РФ, так и в ЕС), так и с целью минимизации рисков от возможных нарушений политик безопасности ИБ и ПДн как функционального подмножества. Анализ защищенности ПДн в настоящее время выполняется формально в соответствии с широким спектром методик, наиболее известные из которых – модели ФСТЭК и комплекса СТО БР ИББС.

В результате анализа НПА и характеристик объектов оценивания сформирована концептуальная модель оценки защищенности ПДн, представленная в форме иерархии и дополненная сравнением объектов относительно стандартов. Эта модель включает многоуровневый классификатор объектов оценивания (построенных на базе перечня «контролей» Приложения А стандарта **ISO/IEC 27001:2005**), систему квалификаторов стандартов (по одной основной шкале – по 3-м уровням значимости), систему нормирования мнений нескольких независимых экспертных групп.

Предложенная модель и методика прошли практическую апробацию в ходе большого количества аудитов ИБ в течение последних 3-х лет и позволяют получать оценки, необходимые для создания эффективных СМИБ, выполняющие, в том числе, требования РФ по защите ПДн.

## Литература


1. Указ Президента РФ 6.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»
2. Федеральный закон РФ 27.07.2006 г. № 152-ФЗ «О персональных данных»
3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России)
4. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации. Банк России, Ассоциация коммерческих банков, 2010 г.
5. Рекомендации в области стандартизации Банка России РС БР ИББС-2.3-2010 «Обеспечение ИБ организаций БС РФ. Требования по обеспечению безопасности ПДн в ИСПДн БС РФ», 2010 г.
6. Рекомендации в области стандартизации Банка России РС БР ИББС-2.4-2010 «Отраслевая частная модель угроз безопасности ПДн при их обработке в ИСПДн БС РФ», 2010 г.
7. ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»
8. ISO/IEC 27005:2008 «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности»
9. ISO/IEC 27000:2009 «Информационные технологии. Методы обеспечения безопасности. Термины и определения»

10. Козин И.Ф., Лившиц И.И. «Информационная безопасность. Интеграция международных стандартов в систему информационной безопасности России» «Информация и связь», № 1, 2010 г.
11. Лившиц И. И. «Проектирование, создание и внедрение комплексных систем обеспечения информационной безопасности на базе международного стандарта ISO/IEC 27001:2005», «Электросвязь», № 4, 2010 г.
12. Лившиц И. И. «Современная практика проведения аудитов ИБ». Сб. трудов 16-я научно-практической конференции «Комплексная защита информации», Республика Беларусь, г. Гродно, 2011 г.
13. Саати Т. «Принятие решений. Метод анализа иерархии». М.: Радио и связь, 1989.
14. Смирнов Э.А. «Управленческие решения». М.: Инфра-М, 2001.

**Лившиц Илья Иосифович** – Ведущий аудитор Ассоциации «Русский Регистр». Область научных интересов: системный анализ, защита информации, риск-менеджмент; Число научных публикаций – 28, в т.ч. числе 9 свидетельств о регистрации программ для ЭВМ, Россия, г. Санкт-Петербург; Эл. Почта: Livshitz_il@Hotbox.ru. Телефон: +7 812 934-48-46. Научный руководитель — А.А. Молдовян.

**Livshitz Ilya** – Lead auditor of Association “Russian Register”. Research interests – System analysis, IT-Security, Risk-management. Number of publications – 28, including 9 Patents of Software. Russia, St. Petersburg, E-mail: Livshitz_il@Hotbox.ru, Phone: +7 812 934-48-46. Scientific advisor – A.A. Moldovyan.

**Молдовян Александр Андреевич** – доктор технических наук, профессор, Заместитель директора СПИИРАН. Область научных интересов: исследование и разработка алгоритмов и средств защиты информации. Число научных публикаций — свыше 100 журнальных статей, более 150 докладов и тезисов, более 50 изобретений, 5 свидетельств о регистрации программ. Maa1305@yandex.ru, СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-5185, факс +7(812)328-4450.

**Moldovyan Alexander** — PhD, professor, Deputy of Director SPIIRAS. Research interests: research and development of algorithms and IT-Security systems. The number of publications — more than 100 articles, more than 150 thesis, more than 50 inventions and 5 software FIPS certificates. Maa1305@yandex.ru, SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-5185, fax +7(812)328-4450

Рекомендовано СПИИРАН, лабораторией проблем информационной безопасности и проблем криптологии, Молдовян А.А., д-р техн. наук, проф.
Статья поступила в редакцию 8.10.2012

## РЕФЕРАТ

*Лившиц И.И.* **Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005**

Обеспечение информационной безопасности (ИБ) ценных информационных активов (в т.ч. персональных данных – ПДн) является одной из ключевых проблем. Современные международные стандарты призваны оптимизировать создание современных систем менеджмента информационной безопасности (СМИБ), отвечающих требованиям как бизнеса, так и требованиям различных регуляторов (т.н. «compliance»). Среди наиболее известных стандартов необходимо отметить прежде всего стандарты ИСО/МЭК серии 27000. Проведенные исследования и практика аудитов ИБ на соответствие требованиям ISO/IEC 27001:2005 показали, что синтез модели оценки защищенности ПДн можно условно разделить на 2 этапа:

***Первый этап*** – сбор информации и идентификация проблемы принятия решения. На этом этапе определяются альтернативы, которые следует изучить в деталях. Далее происходит выбор одного из вариантов решений из множества альтернатив, подготовленных экспертами ранее.

***Второй этап*** – реализация выбранной альтернативы и обобщение опыта, полученного в процессе решения проблемы.

Для решения проблемы сравнения и оценки альтернатив в указанных ситуациях наиболее целесообразен метод сравнения альтернатив относительно стандартов. Исходя из общей структуры критериев и особенностей формирования альтернатив для построения метода оценки защищенности ПДн предлагаются следующие принципы создания модели оценки защищенности ПДн.

*Принцип 1* – приоритет множества критериев перед видом (выбором) последующего метода оценки;

*Принцип 2* – альтернативы определяются (базируются) на экспертных оценках, полученных от независимых групп специалистов.

*Принцип 3* – соответствие количества градаций оцениваемых величин (при формировании списка критериев, перечня альтернатив, матрицы предпочтения стандартов) «доверительному» уровню оценки групп экспертов.

В соответствии с предложенными принципами модель многоуровневой оценки защищенности ПДн состоит из следующих последовательных процедур:

1. Процедура сбора информации (подготовки данных от независимых групп экспертов);
2. Процедура формирования перечня критериев и построение альтернатив;
3. Процедура выборов альтернативы;
4. Процедура оценки и анализ результата.

## SUMMARY

*Livshitz I.I* **The approaches for model's synthesis of private data security assessment in accordance with ISO/IEC 27001:2005 standards requirements.**

Providing information security (IT-Security) and valuable information assets (including "personal data" – PDN) is one of the key issues. Modern International standards are designed for optimization of the creation IT-security management systems (ISMS) that meet both business and other regulators' requirements (so-called «compliance»). Among the most famous ISO standards first of all ISO/IEC Series 27000 should be noted.

The research and practice of auditing information security for compliance with ISO/IEC 27001:2005 have shown that the synthesis model of security assessment PDN can be divided into two stages:

1. The first phase - data collection and identification of a problem of making a decision. At this stage, the alternatives have to be explored in detail. Further, the choice of one of the possible solutions from a variety of alternatives, prepared by experts before has to be made.
2. The second phase - implementation of the chosen alternative and the generalization of experience gained in the process of solving the problem.

Method of comparison of alternatives with standards is the most expedient one for solution of the problem of comparison and evaluation of alternatives in these situations. On the basis of the overall structure of criteria and characteristics of the formation of alternative methods for building security assessment PDN, the following principles for the valuation model of security PDN are proposed

- ✓ Principle 1 - priority of criteria with the kind (choice) of the consequent evaluation;
- ✓ Principle 2 - Alternatives are defined (based) on the experts' opinions obtained from independent groups of experts.
- ✓ Principle 3 – matching of the number of gradations of estimated values (when forming a list of criteria, a list of alternatives, preference matrix standards) to "trust" level of assessment panels.

In accordance with the proposed guidelines, a model of multilevel security assessment PDN consists of the following procedures:

1. Collection of information (training data from independent groups of experts);
2. The procedure for forming a list of criteria and construction alternatives;
3. Procedure of the alternative choice;
4. The evaluation procedure and analysis results.