# ИЕРАРХИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ СООТВЕТСТВИЯ ОРГАНИЗАЦИИ ТРЕБОВАНИЯМ ИБ НА ПРИМЕРЕ СТО БР ИББС-1.2–2014

## A HIERARCHICAL MODEL FOR ASSESSING THE ORGANIZATION'S COMPLIANCE WITH THE REQUIREMENTS OF IB ON THE EXAMPLE OF STO BR IBBS-1.2–2014

***I. Mikhailova***

*Summary.* The article is about the usage of a hierarchical assessment models used by the enterprises to the banking system of the Russian Federation to control the compliance standard of the Bank of Russia on providing information security. The author considers the variants of connection of the assessment model and standard of the information security.

*Keywords:* conformity assessment, information security, information security standards, hierarchical model.

***Михайлова Инна Александровна***
*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*
*i.a.mikhailova@yandex.ru*

*Аннотация.* Настоящая статья посвящена применению иерархической модели оценки, используемой предприятиями банковской системы Российской Федерации в целях контроля соответствия требованиям стандарта Банка России по обеспечению информационной безопасности. Рассмотрены варианты синтеза модели и стандарта по информационной безопасности.

*Ключевые слова:* оценка соответствия, информационная безопасность, стандарты информационной безопасности, иерархическая модель.

Постоянный рост вовлеченности научно-технического прогресса и автоматизации процессов в современную жизнь человечества обуславливает тот факт, что в большинстве сфер деятельности необходимо принимать ключевые решения, опираясь на характеристики, меры, показатели и параметры информационной безопасности.

Банковский сектор несмотря на свою обособленность также подвержен данной тенденции. Это вызвано прежде всего необходимостью обеспечения сохранности информации, представляющей ценность как для банка, так и для их клиентов. Учитывая важность вышеизложенного Банк России проводит активную работу в области соответствия банковской сферы в РФ требованиям СТО БР ИББС-1.0–2014. Одним из ключевых аспектов является корректное понимание и применение методики оценки соответствия информационной безопасности (ИБ) организаций банковской системы Российской Федерации соответствующим требованиям по информационной безопасности.

С целью соответствия множеству параметров и характеристик предприятиям банковской сферы возможно применение иерархической модели соответствия.

Целями при использовании являются стандартизация подходов и способов оценки соответствия обеспечения ИБ организации банковского сектора РФ требованиям СТО БР ИББС-1.0 по следующим направлениям оценки:

- текущий уровень ИБ организации;
- менеджмент ИБ организации;
- уровень осознания ИБ организации.

Основными задачами данной методики являются:

- определение состава показателей ИБ и способов их оценивания;
- определение способа оценивания текущего уровня ИБ организации с помощью установления степени выполнения требований, определенных в разделе 7 СТО БР ИББС-1.0;
- определение способа оценивания менеджмента ИБ организации и уровня осознания ИБ организации с помощью установления степени выполнения требований, определенных в разделе 8 СТО БР ИББС-1.0;
- определения итогового уровня соответствия ИБ организации требованиям СТО БР ИББС-1.0 [1].

Критерии оценки служат для установления значения оценки для конкретного объекта оценки. Критериями оценки ИБ могут являться процедуры ИБ, требования ИБ, сочетание процедур и требований ИБ, а также уровень инвестиций и затрат на ИБ [4].

Свидетельствами оценки ИБ являются записи, изложение фактов или иная информация, имеющая непосредственное отношение к критериям оценки ИБ и являющаяся достоверной. Подобными свидетельствами оценки ИБ являются доказательства выполняемой или

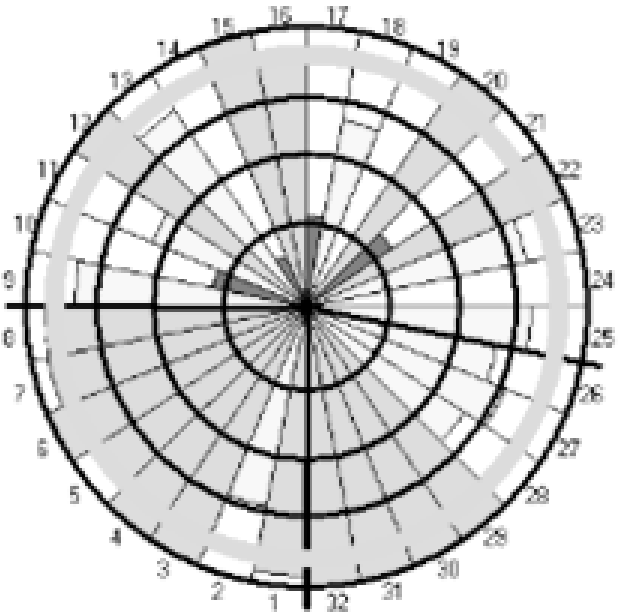

Рис. 1. Свод результатов оценки ИБ иерархическим методом

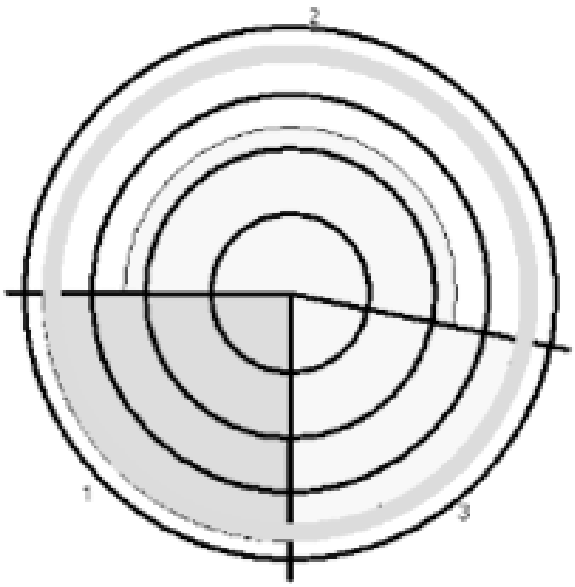

Рис. 2. Итоговое оценивание результатов

проведенной деятельности по обеспечению ИБ в форме отчетных, распорядительных, нормативных документов, а также результатов опросов и наблюдений.

Иерархическая модель — такой вид модели, который использует представление имеющейся в наличии базы данных в виде иерархической структуры. Она, в свою очередь, состоит из объектов различных уровней. Между этими объектами существуют связи, данные каждого объекта могут включать в себя несколько объектов более низкого уровня [4].

Стоит отметить, что иерархические базы данных имеют форму деревьев с дугами-связями и узлами-элементами данных. Иерархия предполагает жесткое подчинение одних данных другим. Использование подобных структур продиктовано тем, что, они удовлетворяют требованиям, стоящим перед оценкой соответствия конкретного банка нормам ИБ банковской сферы.

В целях решения данного вопроса применяются частные и групповые показатели ИБ [3]. Групповые — это определенная структура направлений оценки, предназначенная для детализации оценки как текущего уровня ИБ организации, так и менеджмента, а также уровня осознания ИБ. Оценка групповых показателей (EVMi) требуется в целях получения оценки по существующим в организации направлениям (EV1, EV2 и EV3).

Частные — это некоторая составляющая групповых показателей. Они обозначены в виде вопросов, ответы на которые дают возможность рассчитать оценки, необходимые для формирования оценки EVMi групповых показателей. Каждый вид включает в себя определенный групповой показатель ИБ и все составляющие его частные [2].

Выделим следующие этапы проверки:

- Выявление областей и целей ИБ, которые подлежат проверке;
- Подготовка оценочных материалов для проведения оценки соответствия;
- Процедура оценки соответствия ИБ банка требованиям стандарта;
- Отчет в виде вывода и соответствующие рекомендации.

В результате первоначального анализа определяется перечень информационных систем, применяемых в Банке (в выборку рекомендовано добавлять используемые для реализации платежных, информационных и технологических процессов, а также необходимых для достижения ключевых показателей эффективности и бизнес-целей Банка).

Основные операции над системами, оценка которых выстроена на иерархической модели:

- поиск по базе данных требуемого элемента;
- переход по базе данных — от «дерева» к «дереву»;
- по дереву — от «ветви» к «ветви»;
- переход поэлементно.

Для проведения оценки соответствия применяются:

- анкеты, утвержденные Методикой оценки соответствия информационной безопасности для банковского сектора в РФ;
- источники свидетельств аудита ИБ для оценивания показателя;
- опросные листы.

В результате оценки и в соответствии с методикой определяется сводный результат по параметрам [2].

Результаты оценки соответствия банка используются для составления отчетов и выводов, которые вносят в итоговое подтверждение соответствия. Оно указывает на выполнение / невыполнение СТО БР ИББС-1.0–2014 и формируется используя как полученное аудиторское заключение от внешней организации, так внутренний отчет самооценки банка [1].

В документе необходимо отразить минимальный уровень соответствия, который возможно получить из следующих оценок:

- степени выполнения требований стандарта, регламентирующих обработку персональных данных;
- степени выполнения требований стандарта, регламентирующих защиту персональных данных, в которой не учитываются оценки степени выполнения его требований по обеспечению информационной безопасности с использованием криптографических средств защиты информации;
- группового показателя, отражающего достаточность обеспечения ИБ при использовании криптографических средств защиты информации»;
- итоговый уровень соответствия ИБ банка требованиям стандарта [1, 2].

Таким образом, применение иерархического метода позволяет определить степень соответствия по каждому параметру или характеристике, а также вывести итог по каждому верхнеуровневому значению.

ЛИТЕРАТУРА

1. Стандарт Банка России СТО БР ИББС-1.2–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»
2. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014
3. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, утвержденный приказом председателя Гостехкомиссии России от 19 июня 2002 года № 187
4. В.В. Бахтизин / Метрология, стандартизация и сертификация в информационных технологиях // БГУИР, 2013 г.— 60 с.



Журнал «Современная наука: актуальные проблемы теории и практики»


Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики