

Описание формы предоставления результатов оценки уровня информационной безопасности организаций банковской системы Российской Федерации

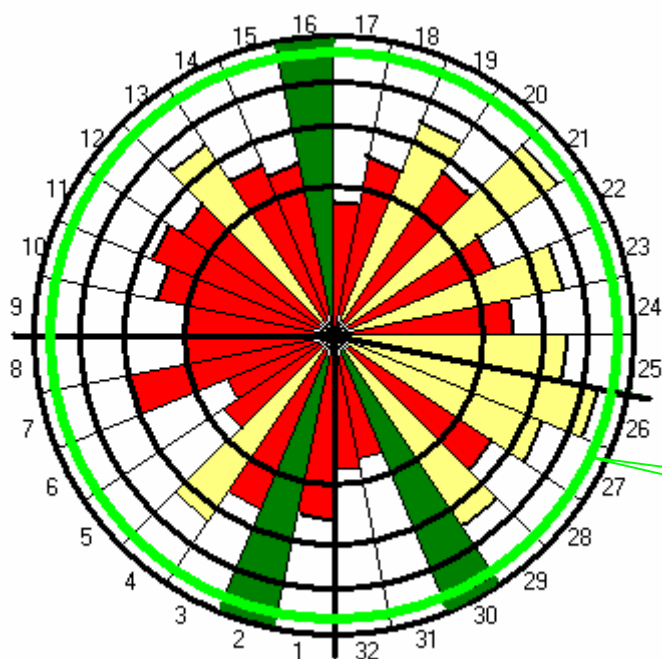
1. Для представления результатов оценки уровня информационной безопасности применяются две цветные диаграммы, отражающие значения групповых показателей и интегральную оценку информационной безопасности организации банковской системы (БС) РФ, проводящей оценку.

На основании интегральной оценки выдается заключение о рейтинге организации в части информационной безопасности.

Групповые показатели

На диаграмме представлены нормированные оценки групповых показателей (32 показателя, перечень и порядок расчета которых приведен в проекте «МЕТОДИКИ ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» (смотри раздел «Методики оценки на соответствие стандартам»)):

Значения групповых показателей



Уровень информационной безопасности организации БС РФ, рекомендуемый стандартом Банка России

Оценка представлена в виде, который соответствует уровням шкалы зрелости стандарта COBIT.

Четвертый уровень зрелости – уровень, рекомендуемый Банком России.

Уровни рейтинга

(соответствуют уровням шкалы зрелости стандарта COBIT)

	0 ур. рейтинга	[0-0.5)
	1 ур. рейтинга	[0.5-0.7)
	2 ур. рейтинга	[0.7-0.85)
	3 ур. рейтинга	[0.85-0.95)
	4 ур. рейтинга	[0.95-1)
	5 ур. рейтинга	[1]

Уровень информационной безопасности организации БС РФ, рекомендуемый стандартом Банка России СТО БР ИББС-1.0-2004

Перечень групповых показателей, представленных на диаграмме:

Таблица 1 – Соответствие групповых показателей ИБ совокупности требований ИБ в областях обеспечения ИБ, представленных в стандарте Банка России

Обозначение групповых показателей ИБ	Наименование групповых показателей ИБ	Разделы стандарта Банка России, содержащие совокупности требований ИБ
M1	Показатель обеспечения ИБ при назначении и распределении ролей и обеспечении доверия к персоналу	8.2.2
M2	Показатель обеспечения ИБ автоматизированных банковских систем на стадиях жизненного цикла	8.2.3
M3	Показатель обеспечения ИБ при управлении доступом и регистрации	8.2.4
M4	Показатель обеспечения ИБ средствами антивирусной защиты	8.2.5
M5	Показатель обеспечения ИБ при использовании ресурсов сети Интернет	8.2.6
M6	Показатель обеспечения ИБ средствами криптографической защиты информации	8.2.7
M7	Показатель обеспечения ИБ банковских платежных технологических процессов	8.2.8
M8	Показатель обеспечения ИБ банковских информационных технологических процессов	8.2.9

Таблица 2 - Соответствие групповых показателей ИБ процессам управления ИБ, представленным в стандарте Банка России

Обозначение групповых показателей ИБ	Наименование групповых показателей ИБ	Пункты стандарта Банка России, соответствующие групповым показателям
M9	Показатель определения/уточнения области действия процессов управления ИБ	9.3, 9.4, 9.5
M10	Показатель оценки рисков ИБ и вариантов минимизации рисков ИБ	9.1, 9.5
M11	Показатель определения/уточнения политики ИБ подразделения Банка России	9.1, 9.5
M12	Показатель выбора/уточнения целей ИБ и защитных мер	9.5
M13	Показатель принятия руководством подразделения Банка России решения о реализации, эксплуатации и совершенствовании процессов управления ИБ	9.1, 9.2, 9.5
M14	Показатель определения плана минимизации рисков ИБ	7.14, 9.1, 9.6
M15	Показатель реализации защитных мер, управления работами и ресурсами	9.1, 9.6
M16	Показатель реализации программы по обучению ИБ	9.1
M17	Показатель обнаружения и реагирования на инциденты ИБ	9.6
M18	Показатель мониторинга и контроля защитных мер	9.7, 11.5

Обозначение групповых показателей ИБ	Наименование групповых показателей ИБ	Пункты стандарта Банка России, соответствующие групповым показателям
M19	Показатель анализа качества процессов управления ИБ	9.7, 9.9
M20	Показатель аудита подразделения Банка России	9.7, 11.1, 11.2, 11.3, 11.4, 11.7
M21	Показатель анализа процессов управления ИБ со стороны руководства подразделения Банка России	9.7
M22	Показатель совершенствования процессов управления ИБ в рамках деятельности службы ИБ	9.8
M23	Показатель совершенствования процессов управления ИБ на уровне руководства подразделения Банка России	9.8
M24	Показатель информирования об изменениях процессов управления ИБ	9.8
M25	Показатель оценки достижимости поставленных целей	9.8

Таблица 3 - Соответствие групповых показателей ИБ базовым и специальным принципам стандарта Банка России

Обозначение групповых показателей ИБ	Наименование групповых показателей ИБ	Пункты стандарта Банка России, соответствующие групповым показателям
M26	Показатель своевременности обнаружения, прогноза развития проблем ИБ и оценки их влияния на цели деятельности подразделения Банка России	6.1.1, 6.1.2, 6.1.3.
M27	Показатель определенности целей, адекватности выбора защитных мер, их эффективности и контролируемости	6.2.1, 6.1.4, 6.1.5, 6.1.8.
M28	Показатель непрерывности обеспечения ИБ и использования опыта	6.1.6, 6.1.7 .
M29	Показатель знания своих клиентов и служащих	6.2.2, 8.2.2.10
M30	Показатель персонификации и адекватности разделения ролей и ответственностей и адекватности ролей функциям и процедурам	6.2.3, 6.2.4, 8.2.2.1
M31	Показатель доступности услуг и сервисов	6.2.5.
M32	Показатель наблюдаемости и оцениваемости обеспечения ИБ	6.2.6.

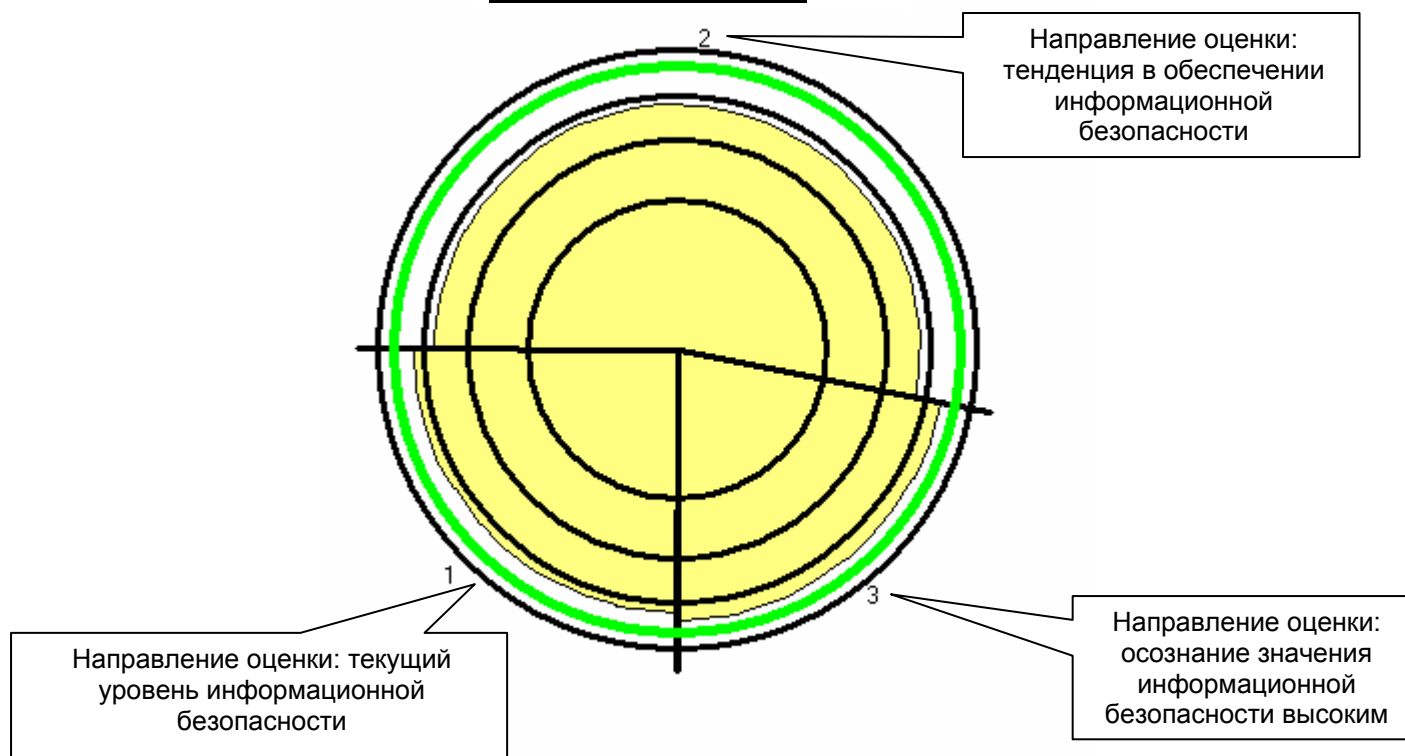
Интегральная оценка

Интегральная оценка по каждому из направлений вычисляется как среднее арифметическое соответствующих групповых показателей ИБ и отображается на круговой диаграмме.

Высший приоритет имеет оценка осознания руководством организации значения ИБ для деятельности (достижения целей бизнеса) организации и оценка тенденции в обеспечении ИБ организации.

Рейтинг организации в обеспечении ИБ не превышает оценки осознания руководством организации значения ИБ для деятельности (достижения целей бизнеса) организации и оценки тенденции в обеспечении ИБ организации, если даже оценка текущего уровня ИБ организации имеет более высокое значение.

Интегральная оценка



Итоговая интегральная оценка информационной безопасности формируется из трех показателей:

- осознание в организации значения ИБ для деятельности (достижения целей бизнеса) организации;
- тенденция в обеспечении ИБ организации;
- текущий уровень ИБ организации.

Итоговая оценка представлена в виде, который соответствует уровням шкалы зрелости стандарта COBIT.

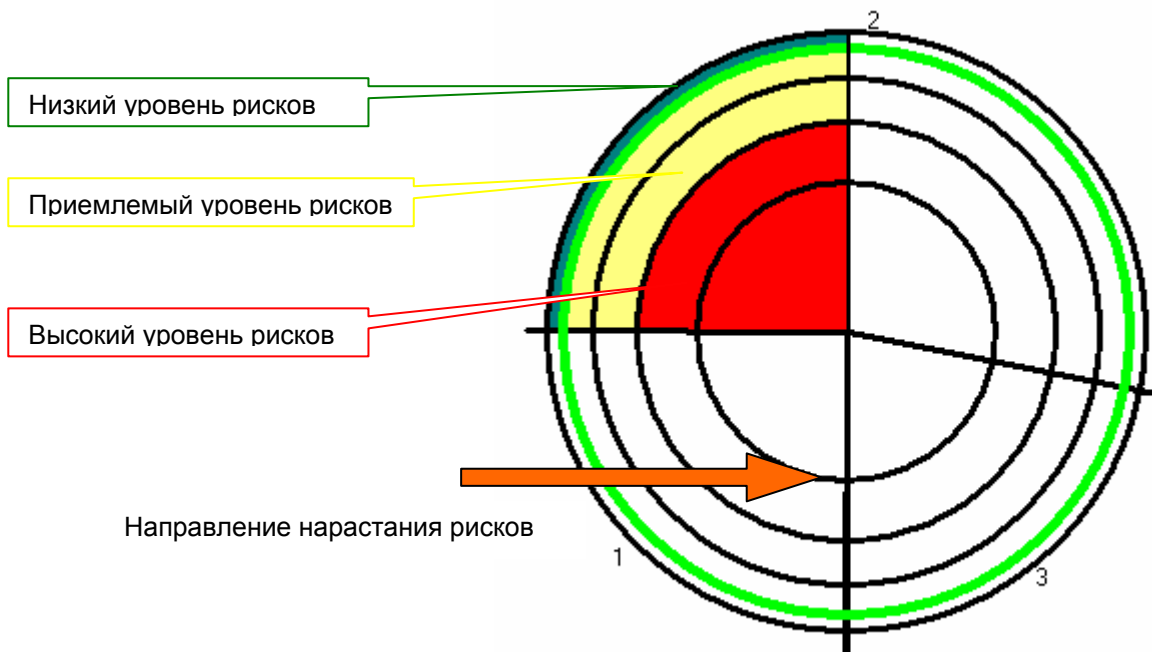
Четвертый уровень зрелости – уровень, рекомендуемый Банком России.

Цветовая легенда

Цветовая легенда: цвета окраски значений отражают уровень рисков – зеленый цвет отражает низкий уровень рисков и высокий уровень информационной безопасности (безусловно положительное заключение), желтый – приемлемый уровень рисков и удовлетворительный уровень безопасности (условно положительное заключение) и красный - высокий уровень рисков и низкий уровень информационной безопасности (отрицательно заключение).

Направление нарастания рисков идет от зеленого к красному.

Цветовая легенда



2. Полное название кредитной организации
3. Кто проводил оценку (полное наименование организации, проводившей оценку на соответствие Стандарту)
4. Методика оценки - название документа
5. Комментарии Банка России: Результат - текущему состоянию уровня информационной безопасности соответствует низкий (приемлемый, высокий) уровень риска.