716-П: Общие положения и основные определения

RTM GROUP

Объединяем IT,
право и безопасность

Далее

СОДЕРЖАНИЕ

01. Операционные риски

Операционный риск – это риск возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов кредитной организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий.

Основной НПА по данному вопросу: Положение Банка России от 8 апреля 2020 г. N 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе"

Требования по 716-П:

Содержатся требования к наполнению ОРД в разрезе порядка управления операционными рисками, контроля его величины, мероприятий по его управлению и оценке.

Сроки выполнения требований по 716-П:

До 01.01.2022.

02. Классификация ОР и Элементы СУОР (п.1.3)

Элементы СУОР согласно п.1.3. включают в себя:

- Процедуры управления операционным риском;
- Классификатор событий операционного риска;
- База событий;
- Контрольные показатели уровня операционного риска;
- Подразделение, ответственное за организацию управления операционным риском;
- Специализированное подразделение;
- Центры компетенций;
- Уполномоченное подразделение;
- Информационная система, обеспечивающая функционирование системы управления ОР и отдельных ее элементов.

02. Классификация ОР и Элементы СУОР.
Дополнительные элементы системы управления ОР (Глава 4)

- Бизнес-процессы организации (п. 4.1.1);
- ОРД (п. 4.1.1-4.1.4);
- Мероприятия по совершенствованию системы управления ОР (п. 4.1.5);
- Мотивация работников по обработке ОР (п. 4.1.6);
- Отчеты по ОР и события ОР (п. 4.1.7-4.2.5, 744-П);*
- Подробный перечень показателей по событиям ОР (п.4.2.4);
- Требования к ИС управления ОР (п. 4.3.1);
- Требования к управлению модельным риском (п. 4.3.2);
- Оценка эффективности системы управления ОР (п. 4.4);
- Плановые (целевые) показатели уровня операционного риска (п. 4.5, п. 3.3 3624-У);
- Ежегодный анализ пересмотра требований по управлению ОР (п.4.6).

* Отчеты формируются в соответствии с № 744-П от 07.12.2020 Положение Банка России «О порядке расчета размера операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением».

02. Классификация ОР и Элементы СУОР.
Операционные риски согласно п 1.4

- Риск информационной безопасности; риск информационных систем;
- Правовой риск;
- Риск ошибок в процессах поддержания работоспособности;
- Риск ошибок в управленческих процессах;
- Риск ошибок в процессах внутреннего контроля;
- Модельный риск;
- Репутационный риск;
- Риск ошибок в процессах управления персоналом.

02. Классификация ОР

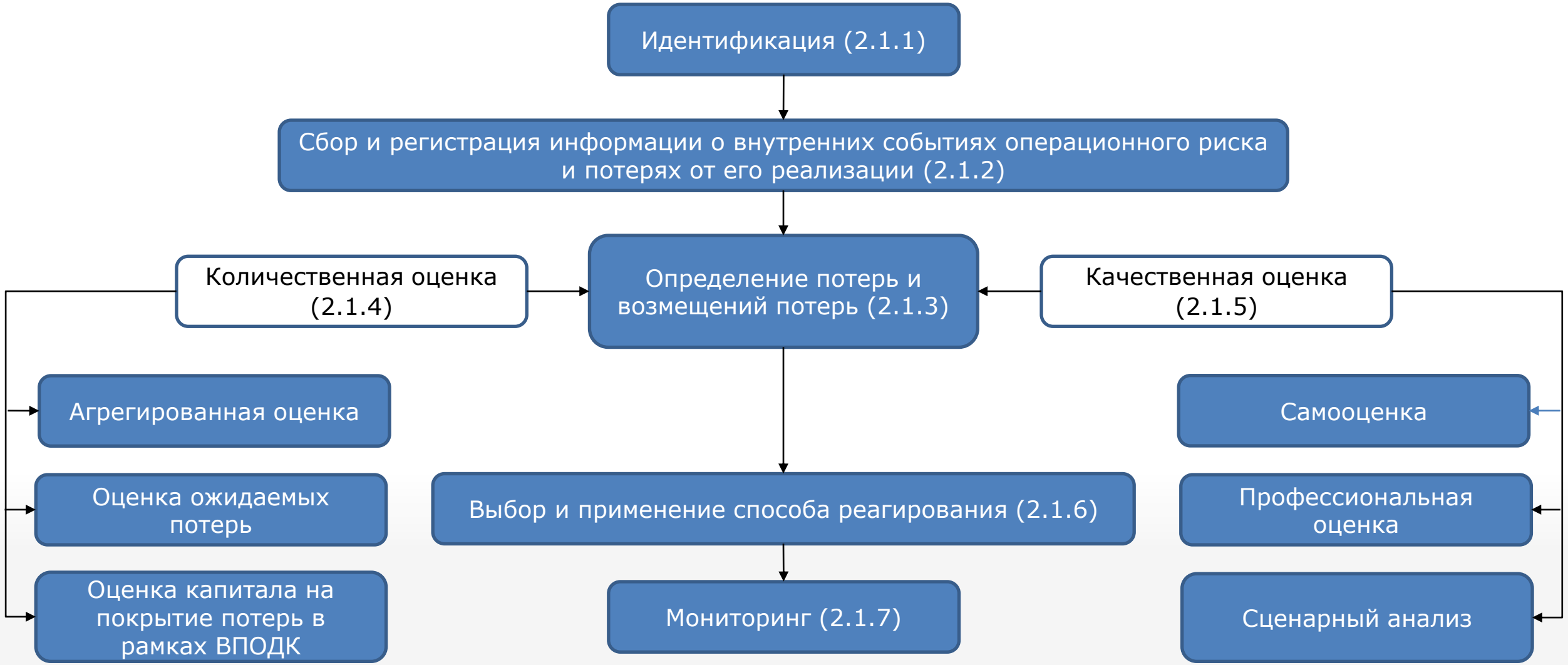
По источникам (п.3.3)

По направлениям деятельности (п.3.9)

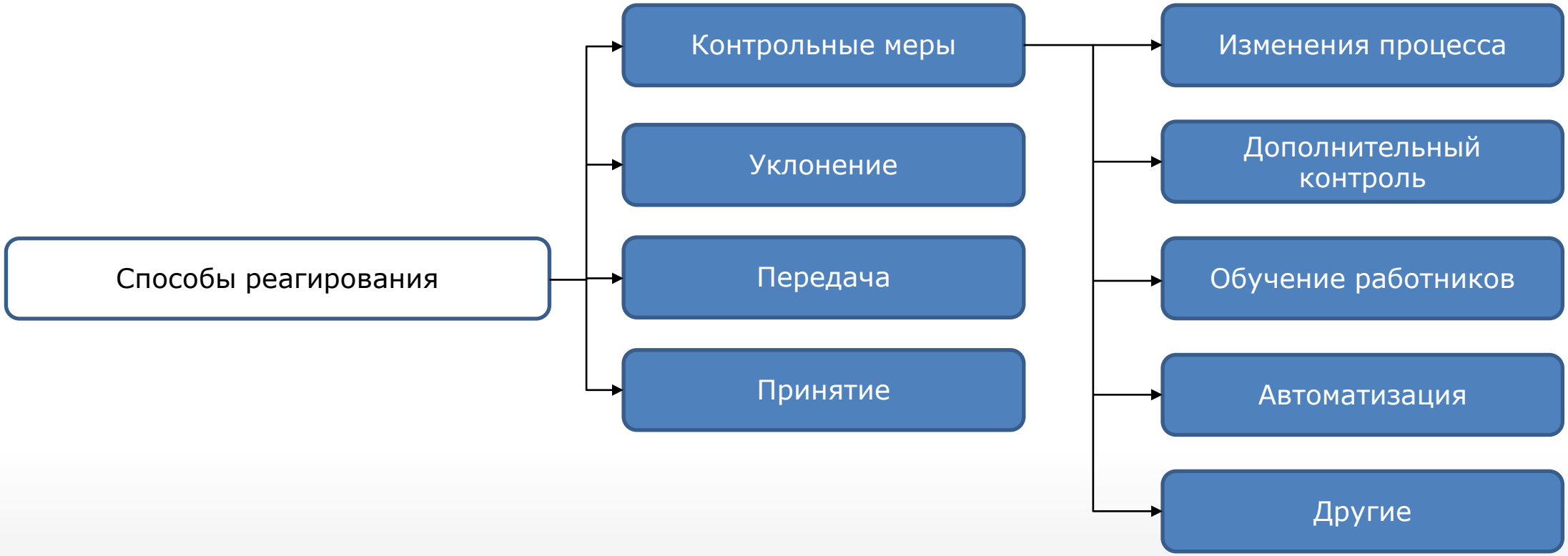
По типам событий (п.3.6, приложение 4)

По видам потерь (п.3.11-3.13)

03. Процедуры управления ОР (Глава 2)



03. Способы реагирования (2.1.6, Приложение 3)



03. Процедуры управления ОР (Глава 2)

Прямые,
отраженные в бухгалтерском учете
(3.12)

Непрямые, не отраженные в бухгалтерском учете
(п.3.13)

- Косвенные, определяемые расчетным методом в денежном выражении
- Качественные, определяются с использованием экспертного мнения
- Потенциальные

03. Процедуры управления ОР.
Контрольные показатели ОР (Глава 5)

Сигнальное (для контроля показателя ответственным подразделением) и контрольное (для контроля советом директоров) значения (п. 5.1).

Утверждение (советом директоров) и расчет значений за 5 лет (п. 5.2-5.3).

03. Процедуры управления ОР.

Подходы к расчету объема капитала на покрытие потерь от реализации ОР

04. База событий (Глава 6)

- Порядок определяется самостоятельно (п. 6.2);
- Порядок учета для распределенных организаций (п. 6.3);
- Пороговые значения (п. 6.5);
- Детализация БС (п. 6.6);
- Нарастающий итого по валовым потерям (п. 6.7);
- Консолидация различных БС (п. 6.10-6.12);
- Возмещение потерь (п. 6.13-6.18);
- Ежегодная независимая оценка сведений в БС (проводится уполномоченным подразделением) (п. 6.19);
- Сохранность и ответственность за ведение данных в БС (п. 6.21).

05. Перечень внутренних документов (типовой) СУОР

- **Политика** управления операционными рисками;
- **Процедуры** управления операционными рисками;
- **Порядок** ведения базы событий операционного риска;
- **Регламент** оценки операционных рисков;
- **Регламент** по расчету объема капитала на покрытие потерь от реализации операционных рисков;
- **План действий,** направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций/

06. Управление риском информационной безопасности

Риск информационной безопасности – риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения ИБ.

Требования: в главе содержатся требования к наполнению ОРД в разрезе порядка управления риском ИБ, контроля его величины, мероприятий по его снижению.

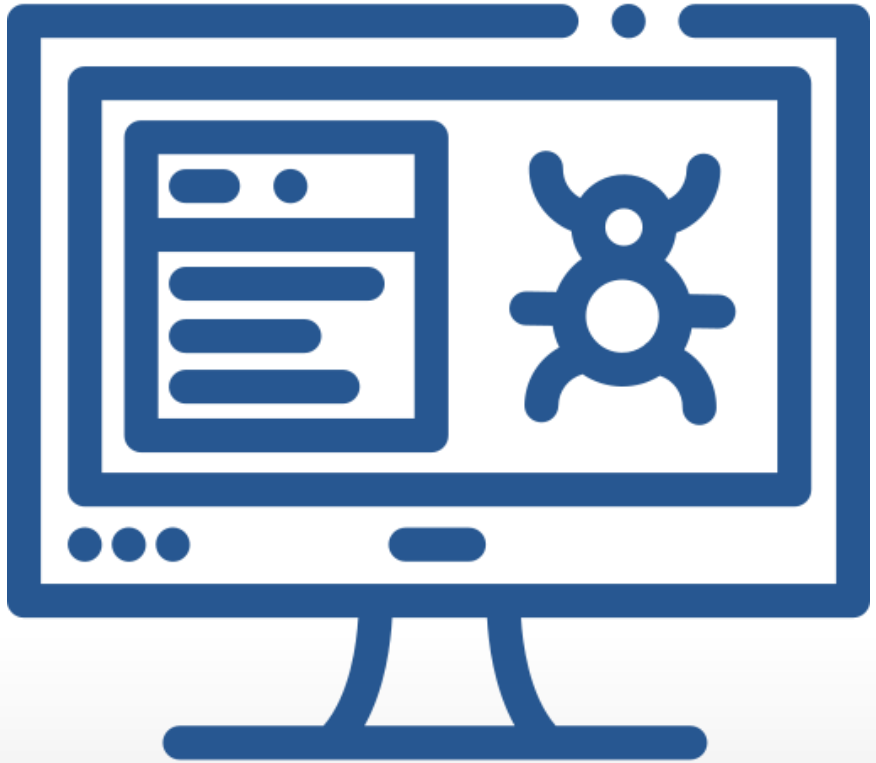
06. Выполнение требований главы 7 «Риски ИБ»

ОРД, которую потребуется скорректировать	ОРД, разработка которой поможет выполнить требования положения
• **Политика ИБ** (в частности *п.7.8)*, должна включать: - функции и ответственность органов и сотрудников в рамках УР ИБ; - сигнальные и контрольные значения уровня риска ИБ; - основные принципы контроля работы СУР ИБ. • **Положение** о службе ИБ. • **Порядок** ведения базы событий ОР.	• **Методика** оценки риска ИБ; • **Регламент** управления риском ИБ; • **Технологическое** описание управления риском ИБ. Среди частных технических требований присутствуют: -Соответствовать общим требованиям 683-П; -Провести тестирование на проникновение; -Провести анализ уязвимостей ПО к ОУД 4.

07. Управление риском информационной системы

Порядок управления риском ИС включает мероприятия по обеспечению требований к непрерывности и качеству функционирования ИС и обеспечению качества данных в ИС.

Требования: Необходимо регламентировать и выполнять мероприятия, обеспечивающие надёжность систем и качество данных.



07. Выполнение требований главы 8 «Риски ИС»

ОРД, которую потребуется скорректировать	ОРД, разработка которой поможет выполнить требования положения
• **Политика ИС** (в частности *п.8.3)*, должна определять: - функции и полномочия ответственного за работу ИС подразделения; - ответственное за работу ИС лицо; - перечень ИС, обслуживающих бизнес-процессы; - требования к ИС; - порядок информационного взаимодействия в рамках реализации политики. • **План** ОНиВД.	• **Регламент** обеспечения качества данных; • **Положение** о службе ИТ; • **Порядок** информационного взаимодействия в рамках управления операционным риском. **Глава содержит** некоторые технические требования, например: - контроль условий эксплуатации ИС и вспомогательного оборудования; - резервное копирование; - тестирование уязвимостей ИС; - регулярные внутренние оценки соответствия.

08. Заключение

Действия по приведению в соответствие требованиям положения **716-П включает в себя:**

Доработку и разработку новой организационно-распорядительной документации.

Изменения в техническом обеспечении.

Дополнения в кадровой организации.

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Андрей Гончаров

Ведущий консультант

RTM Group по информационной безопасности

Кирилл Чекудаев

Ведущий эксперт

RTM Group по управлению рисками

 +7 (495) 197-64-95

 info@rtmtech.ru

 https://rtmtech.ru

 GroupRTM

 rtm.group

 @GroupRtm

 rtm.group.Russia

 t.me/kurilka_ib