Банк России

РЕКОМЕНДАЦИИ УЧАСТНИКАМ ФИНАНСОВОГО РЫНКА ПО КОНЦЕПТУАЛЬНОМУ ДИЗАЙНУ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ»

2026

ОГЛАВЛЕНИЕ

Настоящий материал подготовлен рабочей группой Банка России по вопросам развития систем управления данными участников финансового рынка.

107016, Москва, ул. Неглинная, 12, к. В
Официальный сайт Банка России: www.cbr.ru

Настоящие рекомендации разработаны рабочей группой по вопросам развития систем управления данными участников финансового рынка Банка России в целях создания и совершенствования системы управления данными участников финансового рынка, повышения качества и ценности их данных, повышения эффективности работы с данными.

Каждая организация – участник финансового рынка **самостоятельно принимает решение о необходимости внедрения процесса управления рисками данных**.

Для кредитных организаций (головных кредитных организаций банковской группы) в настоящих рекомендациях **дополнительно** представлены особенности учета событий риска данных в рамках системы управления операционным риском.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Определения и содержание процесса

Риск данных[1] – это вероятность изменения свойств или характеристик качества данных[2], которые могут привести к прямым или непрямым потерям.

Фактор риска данных – условие или недостаток, повышающий вероятность реализации риска данных.

Описание факторов риска данных и их примеров представлено в Приложении 1. Описание примеров по некоторым факторам риска данных представлено в Приложении 2.

Инцидент качества данных – зарегистрированный факт несоответствия данных требованиям к их качеству.

Событие риска данных – событие операционного риска[3], реализация которого связана с инцидентом качества данных[4].

На основе представленных определений участники финансового рынка могут выстроить процесс управления рисками данных.

Для повышения качества управления рисками каждый участник финансового рынка может организовать в рамках системы управления данными процесс управления рисками данных.

Процесс управления рисками данных – непрерывно выполняемый комплекс процедур выявления, оценки и контроля соответствия характеристик качества данных установленным требованиям.

Процесс управления рисками данных реализуется через воронку инцидентов качества данных, где инциденты качества данных при наличии факторов риска данных квалифицируются как события риска данных и при необходимости регистрируются как события операционного риска.

Для кредитных организаций (головных кредитных организаций банковской группы) процесс управления рисками данных интегрируется в систему управления операционным риском с учетом следующих требований.

Кредитные организации (головные кредитные организации банковской группы) при организации системы управления операционным риском[5] соблюдают требования, установленные Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным

---

1 Кредитные организации осуществляют управление риском данных, включая мероприятия и процедуры по обеспечению требований к непрерывности и качеству функционирования информационных систем и обеспечению качества данных в информационных системах, в рамках управления риском информационных систем в соответствии с Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

2 Приложение 2 к Положению Банка России от 02.11.2024 № 845-П «О порядке расчета величины кредитного риска банками с применением банковских методик управления кредитным риском и моделей количественной оценки кредитного риска».

3 Для кредитных организаций (головных кредитных организаций банковской группы) в значении, установленном в пункте 1.2 Положения Банка России № 716-П.

4 Кредитные организации (головные кредитные организации банковской группы) обеспечивают учет событий операционного риска в соответствии с требованиями Положения Банка России № 716-П.

5 В том числе в части идентификации операционного риска, ведения базы событий, управления риском информационных систем (включая требования к обеспечению качества данных).

риском в кредитной организации и банковской группе» (далее – Положение Банка России № 716-П).

Согласно Положению Банка России № 716-П, риск данных не выделен в самостоятельную категорию операционного риска. Риск данных необходимо классифицировать как операционный риск с точки зрения его возникновения, в соответствии с определением операционного риска согласно пункту 4.1 главы 2 Приложения 1 к Указанию Банка России от 15.04.2015 № 3624-У[6], а также требованиями[7] к процессу управления рисками в рамках внутренних процедур оценки достаточности капитала (ВПОДК).

Для эффективного контроля риска данных необходима адаптация процедур управления операционным риском с учетом специфики жизненного цикла данных.

Кредитные организации (головные кредитные организации банковской группы) в части организации сбора и регистрации событий операционного риска осуществляют ведение базы событий операционного риска в соответствии с требованиями Положения Банка России № 716-П. При этом в базе событий операционного риска кредитной организации (головной кредитной организации банковской группы) допускается введение дополнительных признаков (связей) с инцидентами качества данных.

Решение о необходимости внедрения процесса управления рисками данных может основываться на финансовых, операционных и репутационных критериях, характере обрабатываемых данных, уровне зрелости системы управления данными, а также иных важных для организации факторах. Возможные критерии целесообразности внедрения процесса «Управление рисками данных» применительно к участникам финансового рынка представлены в табл. 1.

КРИТЕРИИ ЦЕЛЕСООБРАЗНОСТИ И ГОТОВНОСТИ К ВНЕДРЕНИЮ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 1*

Группа критериев	Критерии целесообразности и готовности организации к внедрению процесса «Управление рисками данных»
Критерии целесообразности	
Финансовые критерии	**1. Превышение лимита операционных потерь от ошибок в данных.** В расчет могут включаться: прямые потери от ошибочных инвестиционных, кредитных, торговых решений, принятых на основе неполных или ошибочных данных, а также компенсационные выплаты клиентам по претензиям, связанным с ошибками в обработке данных. Пример: «совокупные потери от некачественных данных за календарный год превысили установленный лимит (0,1% от чистого операционного дохода организации)». **2. Существенность корректировок значений показателей финансовой отчетности.** Пример: «корректировки значений показателей публичной отчетности, связанные с ошибками в исходных данных, повлекли необходимость пересмотра (повторного выпуска) публичной отчетности / превысили 5% от чистой прибыли». **3. Потеря доходов от неоптимальных решений.** Пример: «использование некачественных данных при принятии инвестиционных, кредитных или иных решений привело к снижению доходности портфеля более чем на 10 базисных пунктов по сравнению с потенциально достижимой при использовании корректных данных»

[6] См. пункт 4.1 главы 2 Приложения 1 Указания Банка России от 15.04.2015 № 3624-У (ред. от 06.10.2023) «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы».

[7] Согласно главе 2 Указания Банка России от 15.04.2015 № 3624-У (ред. от 06.10.2023) «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы».

Группа критериев	Критерии целесообразности и готовности организации к внедрению процесса «Управление рисками данных»
Операционные критерии	**1. Рост затрат* на устранение ошибок в данных.** Пример: «расходы на выявление и устранение ошибок в данных, включая дополнительные часы работ сотрудников, вовлечение внешних консультантов, доработку ИТ-систем, превысили 2% от ИТ-бюджета / показали годовой рост более 20% при сопоставимом объеме операций». **2. Рост частоты сбоев в критических бизнес-процессах.** Пример: «более 5% сбоев в критических бизнес-процессах за последний квартал были вызваны проблемами с качеством данных». **3. Длительное время устранения инцидентов качества данных.** Пример: «среднее время устранения инцидентов качества данных превысило 4 часа для критичных процессов, 24 часа для некритичных процессов». **4. Высокая зависимость от ручных проверок качества данных.** Пример: «более 30% проверок качества критичных данных (CDE) были выполнены вручную»
Репутационные критерии	**1. Рост количества клиентских жалоб на ошибки в данных.** Пример: «количество обоснованных жалоб клиентов на ошибки в их персональных данных и выписках превысило значение прошлого года на 50%». **2. Появление публичных инцидентов качества данных.** Пример: «в 2025 году произошел инцидент качества данных, получивший освещение в СМИ или социальных сетях, негативно повлиявший на репутацию организации и/ или потребовавший публичных извинений». **3. Рост оттока клиентов из-за проблем с данными.** Пример: «более 5% ушедших клиентов в качестве основной причины ухода указали на ошибки в данных, некорректные расчеты и проблемы с качеством сервиса»
Пререквизиты (критерии зрелости) к внедрению процесса	
Критерии организационной готовности	**1. Назначен Руководитель службы управления рисками.** В организации выделено функциональное направление по управлению рисками и назначен его руководитель. **2. Выделение управления данными в самостоятельный вид деятельности.** Управление данными формально выделено как отдельная функция в организационной структуре, с закрепленными процессами, ответственными и ресурсами. **3. Разработана политика управления данными организации.** Разработан базовый документ, охватывающий аспекты жизненного цикла данных. Допускается, что политика может быть утверждена на уровне одного из комитетов организации. **4. Определены и назначены Владельцы данных.** Частично произведено и/или продолжается назначение Владельцев данных за критичные элементы данных (CDE). На начальном уровне Владельцы данных могут быть назначены для наиболее критичных областей. **5. Владельцами данных произведена оценка критичности данных.** Разработана методика оценки критичности данных для бизнес-процессов, которую Владельцы данных могут применять самостоятельно. На основе методики Владельцы данных, с учетом оценки критичности бизнес-процессов и их функций, определяют критичность данных
Критерии процессной зрелости (внедрены и функционируют процессы)	**1. Закреплена ответственность за данные.** Определены Владелец данных и другие роли (по необходимости), начата разработка правил и процедур по управлению данными, запущены первые проекты/инициативы по управлению данными. **2. Качество данных.** Систематически ведется работа по оценке и улучшению качества критичных данных

** Конкретные значения роста затрат участник финансового рынка определяет самостоятельно.*

1.2. Модель процесса «Управление рисками данных»

Участнику финансового рынка рекомендуется организовывать управление риском данных как подвидом риска информационных систем в соответствии с Приложением 3.

Общее описание модели управления риском данных

Целевая модель управления рисками данных представляет собой структурированную систему взаимодействия между системой управления данными (далее – СУД) и системой управления рисками (далее – СУР) организации. Модель базируется на принципе воронки рисков данных, обеспечивающем последовательную трансформацию первичной информации об инцидентах качества данных в управляемые риски.

Источниками риска данных являются не только инциденты, связанные с качеством данных, но и выводы проверок (внутренних/внешних), предписания Банка России, изменения законодательства, которые фиксируются как события риска данных.

Основными компонентами модели управления риском данных являются:

1. Риск данных.
2. Событие риска данных.
3. Инцидент качества данных.
4. Ключевые индикаторы риска данных (КИРД).
5. Мероприятия по снижению риска данных.

Принципы функционирования модели управления риском данных

Модель реализует принцип воронки инцидентов качества данных, поэтапно отбирая из множества инцидентов те, которые идентифицируются и свидетельствуют о материализации события риска данных.

На входе процесса системы управления данными организации фиксируется поток инцидентов качества данных, включающий не только технические нарушения, но и результаты внутренних и внешних проверок, предписания регуляторов, изменения законодательства. Каждый инцидент качества данных проходит процедуру оценки. Для оценки масштаба распространения и критичности затронутых данных рекомендуется использовать документацию по потокам данных (Приложение 4).

При подтверждении критериев существенности инцидент качества данных квалифицируется как событие риска данных и далее регистрируются в системе управления рисками.

Ключевым элементом модели является механизм связывания (указание ссылки на уникальный идентификатор – ID риска) события риска данных с карточками рисков в Реестре операционных рисков через соответствующий идентификатор (ID риска). Каждое событие риска данных должно быть связано минимум с одной карточкой риска через уникальный идентификатор, при этом допускается множественная связь для комплексных событий риска данных. Карточка риска агрегирует статистику по всем связанным событиям риска данных, обеспечивая накопление базы знаний для совершенствования системы управления данными.

На основе агрегированной информации по рискам данных и значениям КИРД инициируются установленные процедуры реагирования на выявленные инциденты качества данных, разрабатываются корректирующие и предупреждающие мероприятия, а также осуществляется контроль их исполнения и оценка эффективности в рамках общей системы управления рисками.

Распределение ответственности между СУД и СУР[8]

Распределение функций по управлению риском данных между СУД и СУР осуществляется организацией самостоятельно с учетом уровня зрелости указанных функций, наличия необходимых компетенций и профильности деятельности соответствующих подразделений, сложившихся практик и особенностей организационной структуры.

При распределении зон ответственности рекомендуется обеспечивать разграничение функций (мониторинг и выявление инцидентов качества данных, оценку, анализ первопричин и выработку корректирующих мер), исключая дублирование и обеспечивая целостность процесса управления риском данных. При этом должны быть учтены каскадные эффекты – влияние проблем с данными на кредитные, рыночные и иные виды рисков организации.

---

[8] Для кредитных организаций (головных кредитных организаций банковской группы) требования к участникам процесса управления операционным риском установлены нормами Положения Банка России № 716-П.

Независимо от выбранной организационной структуры и модели распределения функций, организация обеспечивает соответствие требованиям к управлению рисками данных согласно нормативным актам Банка России.

1.3. Общие правила по работе с рисками данных

Принципы идентификации рисков данных

Управление рисками данных основывается на проактивном подходе к выявлению угроз при использовании данных в бизнес-процессах организации. Идентификация включает определение как прямых последствий, так и косвенных – каскадных эффектов от распространения некорректных данных между системами.

Характеристики качества данных с точки зрения управления рисками данных определяются Владельцем данных и/или бизнес-процессов, которому могут оказывать поддержку сотрудники, назначенные на роли в СУД и СУР. СУД производит выявление и фиксацию инцидентов качества данных на основе установленных Владельцем данных и/или бизнес-процессов характеристик качества данных, первичную квалификацию причин возникновения ошибок данных.

Анализ первопричин нарушений качества данных рекомендуется проводить систематически с использованием методологии выявления корневых причин. По результатам анализа целесообразно устанавливать взаимосвязи факторов риска данных с критичными бизнес-процессами и оценивать уязвимости в цепочках движения данных и контрольных процедурах.

Критерии оценки и квалификации рисков данных

Инциденты качества данных подлежат комплексной оценке, включающей:
1. Анализ системности причин и вероятности повторения.
2. Влияние на непрерывность бизнес-процессов.
3. Оценку соответствия нормативным требованиям.

При подтверждении системного характера и превышении порога регистрации инцидент качества данных квалифицируется как событие риска данных. Пороги существенности устанавливаются СУР организации самостоятельно с учетом риск-аппетита и регуляторных требований.

Превентивная идентификация рисков данных

Помимо реактивного реагирования на инциденты качества данных, обязательна ежегодная самооценка подверженности рискам данных. Владельцы и потребители данных анализируют следующие параметры:
1. Полнота охвата проверками качества данных.
2. Изменения в процессах и системах.
3. Накопление технического долга по ИТ-архитектуре.
4. Пороги существенности по инцидентам качества данных и значениям КИРД.
5. Изменения регуляторных требований.

Приоритизация рисков данных

1. Приоритет определяется комбинацией факторов:
2. Критичность влияния на потребителей данных.
3. Вероятность реализации.
4. Степень взаимосвязанности с другими процессами организации.
5. Значимость для регуляторной отчетности и выполнения регуляторных требований.

Особое внимание уделяется факторам риска данных, влияющим на регуляторную отчетность, клиентские операции и требования ПОД/ФТ, то есть на вероятность реализации регуляторного риска и риска ошибок в процессах осуществления внутреннего контроля.

Организация мониторинга риска данных

Мониторинг риска данных[9] осуществляется с учетом следующих особенностей:

Оперативный (ежедневно), в том числе:
- отслеживание инцидентов качества данных и их квалификация как событий риска данных;
- контроль устранения выявленных нарушений качества данных.

Тактический (ежемесячно-ежеквартально):
- анализ причин и последствий событий риска данных;
- актуализация карточек рисков данных;
- актуализация алгоритмов расчета и порогов срабатывания по КИРД.

Стратегический (ежегодно):
- оценка эффективности системы управления риском данных;
- анализ результативности планов митигации[10];
- формирование рекомендаций по развитию процесса управления рисками данных.

Рекомендуется вести базу знаний по событиям риска данных для совершенствования системы управления данными и обоснования инвестиций в качество данных.

Документирование и отчетность

Рекомендуется все выявленные события риска данных вносить в Реестр операционных рисков (если его ведение предусмотрено в организации)[11], а также обеспечить формирование регулярных отчетов, консолидирующих данные о ходе управления операционным риском. Отчеты могут включать анализ зафиксированных инцидентов качества данных, оценку динамики контрольных показателей уровня риска и информацию о выполнении мероприятий по обеспечению качества данных.

---

[9] Кредитные организации (головные кредитные организации банковской группы) выполняют процедуру мониторинга операционного риска в соответствии с подпунктом 2.1.7 пункта 2.1 Положения Банка России № 716-П.

[10] Под митигацией в документе понимается комплекс превентивных мер по снижению вероятности реализации и/или минимизации последствий риска данных до приемлемого уровня.

[11] Кредитные организации (головные кредитные организации банковской группы) в части организации сбора и регистрации событий операционного риска осуществляют ведение базы событий операционного риска в соответствии с требованиями Положения Банка России № 716-П. При этом в базе событий операционного риска кредитной организации (головной кредитной организации банковской группы) допускается введение дополнительных признаков (связей) с инцидентами качества данных.

1.4. Внедрение процесса «Управление рисками данных»

Процесс управления рисками данных внедряется **поэтапно в соответствии с уровнем зрелости** системы управления данными и системы управления рисками организации. Ниже описаны подходы к внедрению процесса «Управления рисками данных» от начального уровня зрелости до уровня операционализации. Описание подхода на уровень трансформации выходит за рамки настоящего документа, поскольку предполагает значительную вариативность подходов, определяемую стратегическими приоритетами и культурными особенностями организации.

Начальный уровень зрелости СУД

Начало процесса: управление рисками данных в организации не осуществляется или осуществляется разрозненно, без интеграции в общую систему управления рисками организации, имеет место фрагментарный контроль качества данных, отсутствует систематический учет инцидентов качества данных, риски данных не выделены в управленческой отчетности.

Ключевые действия по внедрению модели:
1. Создание механизма фиксации инцидентов качества данных в едином журнале или реестре.
2. Разработка критериев оценки существенности событий риска данных.
3. Формирование подраздела «Риски данных» в Реестре операционных рисков (если ведение реестра операционных рисков предусмотрено в организации).
4. Учет рисков данных в политиках, стандартах, регламентах работы организации.
5. Назначение ответственных за первичную оценку рисков среди Владельцев данных.

Результат внедрения: реализован ряд инициатив по созданию базового механизма выявления, оценки и донесения до руководства о рисках данных. Заложена основа для развития процесса на следующих уровнях зрелости. Самооценка уровня зрелости системы управления данными[12] соответствует или превышает зрелость «2 – уровень осознания».

СУД на уровне 2 – «осознание»

Начало процесса: ведутся отдельные инициативы и/или проекты по интеграции управления рисков данных в общую систему управления рисками, налажен учет инцидентов качества данных, определено большинство Владельцев данных, ведется инвентаризация критичных данных. Служба управления рисками может вести реестр операционных рисков данных, если это предусмотрено в организации.

Ключевые действия по настройке модели:
1. Внедрение процедуры трансформации инцидентов качества данных в события риска данных.
2. Установление связей между событиями риска данных и рисками данных через соответствующие идентификаторы (указание в событии риска данных уникального идентификатора – ID риска).
3. Интеграция с процессами управления операционными рисками организации.
4. Формирование КИРД для мониторинга и определение их порогов.

Результат внедрения: управление рисками данных частично интегрировано в общую СУР. Применяются единые принципы и методологии оценки и обработки рисков. Самооценка уровня зрелости соответствует или превышает зрелость «3 – уровень применения».

---

[12] Используя «Методику оценки зрелости систем управления данными участников финансового рынка».

СУД на уровне 3 – «применение»

Начало процесса: процессы управления риском данных частично интегрированы в систему управления рисками данных, формализованы, внедрены инструменты мониторинга, определена критичность данных для бизнес-процессов. Регулярно осуществляются идентификация и оценка рисков данных.

Ключевые действия по развитию модели:

1. Автоматизация сбора и классификации инцидентов качества данных с использованием ИТ-инструментов.
2. Реализация двусторонней интеграции между СУД и СУР на уровне данных.
3. Внедрение предиктивной аналитики для прогнозирования рисков.
4. Связывание рисков данных с бизнес-процессами и системами в едином репозитории.
5. Интеграция с процессами обеспечения непрерывности деятельности и управления риском аутсорсинга[13].
6. Проведение регулярной самооценки рисков данных и реализация мер по митигации рисков.

Результат внедрения: управление рисками данных полностью интегрировано в общую систему управления рисками. Обеспечен баланс между операционной эффективностью и контролем рисков. Регулярно проводится самооценка рисков данных. Организация способна принимать обоснованные риск-ориентированные решения в области управления данными с учетом стоимости риска и затрат на его митигацию. Самооценка уровня зрелости СУД соответствует зрелости «4 – уровень операционализации» или превышает ее.

[13] Рекомендуется распространить требования Политики управления данными на процессы взаимодействия с аутсорсерами и планирования непрерывности деятельности. В рамках этой работы рекомендуется:
– при оценке рисков аутсорсинга анализировать системы хранения и защиты данных подрядчика, а также его способность к восстановлению информации после сбоев;
– в сценариях обеспечения непрерывности включать проверки резервного копирования и восстановления не только внутренних, но и внешних (аутсорсинговых) сервисов;
– внедрить механизм регистрации инцидентов, при котором сбой доступности данных у аутсорсера классифицируется одновременно как событие риска аутсорсинга, риска нарушения непрерывности и риска данных (для кредитных организаций (головных кредитных организаций банковской группы) – в соответствии с Положением Банка России № 716-П).

2. КОНЦЕПТУАЛЬНЫЙ ДИЗАЙН ПРОЦЕССОВ СУД

Концептуальный дизайн разработки любого процесса СУД предваряется карточкой процесса, которая представляет краткое описание основных составляющих процесса и включает следующие разделы:

1. Цели процесса.
2. Участники процесса.
3. Объекты управления.
4. Требования к процессу.
5. Методы, обеспечивающие процесс.
6. Показатели эффективности процесса.
7. Контрольные процедуры.

За карточкой процесса в концептуальном дизайне процесса следует описание процедуры организации эффективного процесса и зон ответственности в нем.

Описание организации эффективного процесса включает следующие разделы:

1. Сводная таблица организации процесса.
2. Типовые проблемы и способы их решения (приложения к рекомендациям).

Описание организации зон ответственности в процессе происходит в виде матрицы RACI[1].

2.1. Описываемые процессы

В рекомендациях Банка России по развитию системы управления данными участников финансового рынка представлены концептуальные основы построения процессов СУД. Указанные концептуальные основы применяются при проведении самооценки зрелости СУД участников финансового рынка[2], а именно[3]:

1. Руководство данными.
2. Качество данных.
3. Архитектура и моделирование данных.
4. Управление метаданными.
5. Справочные и основные данные.
6. Интеграция данных.
7. Управление рисками данных.

2.2. Описание разделов карточки процесса

1. Цели процесса

В разделе описываются основные цели, которые должны быть достигнуты в результате выполнения процесса. Цели формулируются таким образом, чтобы отразить желаемое состояние данных и их использование в организации. Примерами целей могут быть обеспечение качества

[1] Матрица RACI, или матрица ответственности, – инструмент для управления отношениями в команде.

[2] Согласно «Методике оценки зрелости систем управления данными участников финансового рынка».

[3] Рабочая группа по развитию систем управления данными участников финансового рынка проводит оценку целесообразности реализации рекомендаций «Безопасность данных», «Хранилища данных и бизнес-аналитика» и «Хранение и операции с данными». В ходе анализа учитывается наличие действующих нормативных актов, рекомендаций и практических руководств, охватывающих соответствующую проблематику.

данных, повышение доступности данных, соблюдение регуляторных требований в отношении данных и тому подобное.

2. Участники процесса

В этом разделе указываются роли сотрудников организации для конкретного процесса СУД. Четкое распределение ролей и обязанностей является важным условием эффективного выполнения процесса СУД (подраздел 2.3 «Рекомендаций участникам финансового рынка по построению эффективной системы управления данными»).

3. Объекты управления

Здесь указываются объекты управления в процессе СУД. Объектами управления могут быть данные (структурированные и неструктурированные), метаданные, потоки данных, системы хранения данных и так далее.

Для каждого объекта управления приводится краткое описание его характеристик, способов идентификации и учета. Определение объектов управления позволяет установить границы процесса, обеспечивать и контролировать полноту функции управления, учитывать перевод из одного качественного или количественного состояния в другое.

4. Требования к процессу

В этом подразделе указываются рекомендации (требования) к процессу управления данными, которым должен соответствовать рассматриваемый процесс. Требования связаны с разработкой, наличием артефактов, соблюдением стандартов и регуляторных норм, производительностью процесса, качеством результатов и так далее.

Перед внедрением требований целесообразно провести следующие мероприятия:
1. Самооценка зрелости СУД. Это позволит понять текущий уровень зрелости СУД, выявить области для улучшения и постановки новых требований.
2. Определение операционной модели СУД, плана поддержки проектов и оценки соответствия нормативно-правовым требованиям.
3. Разработка стратегии управления данными, которая должна включать цели, задачи и приоритеты развития СУД, согласованные с бизнес-целями и (или) стратегией организации.

На этапе реализации требований к процессам нужно учитывать организационные особенности, такие как структура компании, существующие бизнес-процессы и культурные аспекты. Например, распределение ролей и ответственности должно быть четко определено и закреплено за конкретными сотрудниками или отделами.

Важно учесть взаимодействие между различными функциями и департаментами для обеспечения согласованности и эффективности процессов управления данными.

Для проверки того, что требования учтены и внедрены правильно, необходимо установить контрольные процедуры и индикаторы. Мониторинг и контроль должны осуществляться постоянно и включать регулярное обновление и пересмотр политики и процедур управления данными. Следует уделить особое внимание обучению и развитию сотрудников в области управления данными. Проведение регулярных тренингов и семинаров позволит повысить уровень осведомленности и компетентности сотрудников.

5. Методы, обеспечивающие процесс

Раздел посвящен описанию основных методов, которые используются для выполнения этого процесса управления данными. Методы могут включать разработку стандартов, моделирование данных, профилирование данных, оценку качества данных и так далее.

Для каждого метода в дальнейшем приводится краткое описание его сути и ожидаемых результатов. Выбор и применение адекватных методов для организации является важным фактором успешной реализации процессов СУД.

6. Показатели эффективности процесса

Для каждого метода, обеспечивающего процесс, должен существовать соответствующий показатель.

Рекомендации по использованию показателей:

1. Адаптируйте показатели к специфике вашей организации и ее целям в области управления данными.
2. Обеспечьте наличие надежных источников данных для расчета показателей.
3. Используйте комбинацию показателей для получения полной картины эффективности управления данными.
4. Регулярно отслеживайте и анализируйте значения показателей, чтобы выявлять тенденции и области для улучшения.
5. Установите целевые значения для каждого показателя и сравнивайте фактические результаты с целевыми значениями.
6. Используйте результаты анализа показателей для принятия обоснованных решений и разработки планов по улучшению практики руководства данными.
7. Регулярно пересматривайте и обновляйте показатели, чтобы они оставались актуальными и соответствовали меняющимся потребностям организации.
8. Обеспечьте прозрачность и доступность информации о показателях для всех заинтересованных сторон, чтобы стимулировать их вовлеченность и инициативы по управлению данными.
9. Интегрируйте показатели в общую систему управления эффективностью организации и свяжите их с ключевыми показателями эффективности.

7. Контрольные процедуры эффективности процесса

Контрольные процедуры – это процедуры, связанные с показателями эффективности процесса, которые используются для мониторинга и оценки выполнения процесса СУД. Регулярное выполнение контрольных процедур позволяет своевременно выявлять и устранять трудности в организации СУД.

2.3. Описание организации процесса

Организация процесса представляется в виде сводной таблицы. В ней описывается целостное представление о ключевых элементах организации процесса (требованиях, методах) и, если возможно, указываются соответствующие им показатели эффективности процесса и контрольные процедуры.

Каждая строка требований демонстрирует взаимосвязи между различными аспектами процесса и позволяет обеспечить его комплексную реализацию, оценку эффективности и контроль за его

соблюдением. Сводную таблицу организации процесса можно использовать при внедрении или оптимизации процесса, а также для обучения сотрудников.

Использование сводной таблицы способствует выбору подходящих методов и средств для эффективной реализации процесса, определению целевых показателей эффективности и планированию мероприятий по контролю за эффективностью процесса.

В организацию процесса входит также описание типовых проблем и способов их решения. В этом разделе описывается опыт в области решения типовых проблем, возникающих в ходе выполнения процесса.

Приведенные примеры содержат наиболее распространенные проблемные ситуации, а также проверенные на практике способы их разрешения.

Названные способы призваны способствовать повышению эффективности управления процессом. Описание типовых проблем можно использовать для диагностики и устранения проблем в процессе, а также для предотвращения их возникновения. Описание проблемной ситуации помогает идентифицировать ее, найти или синтезировать подходящий вариант решения.

2.4. Описание организации зон ответственности (матрица RACI) в процессе

Матрица ответственности RACI используется для структурирования зон ответственности в сложных процессах. Это необходимо для четкого установления обязанностей по 4 категориям:

1. Исполнитель задачи/подзадачи проекта.
2. Ответственный за задачу – тот, кто ставит задачи исполнителям. Важно, чтобы у одной задачи был только один ответственный.
3. Консультант по экспертным вопросам.
4. Информируемый – тот, кто должен быть в курсе выполнения задачи и (или) ее результатов.

2.5. Использование концептуального дизайна для разработки процессов СУД

Развитие СУД организации должно быть обоснованным с позиции принципа разумной целесообразности. Для этого предлагается рассмотреть обобщенный клиентский путь сотрудника организации, решающего аналитическую задачу на данных.

Рассмотрим внедрение процессов СУД в контексте обобщенного пути пользователя, решающего аналитическую задачу (рис. 1).

Этот путь состоит из нескольких ключевых этапов: появление бизнес-идеи и потребности в данных, поиск данных, сбор данных, использование данных и предоставление результата. На каждом из этих этапов внедрение соответствующих процессов СУД может принести существенную пользу.

Для каждого этапа клиентского пути есть релевантные задачи процессов управления данными. Например, на этапе появления бизнес-идеи определяется потребность в данных, за которой следует постановка задачи.

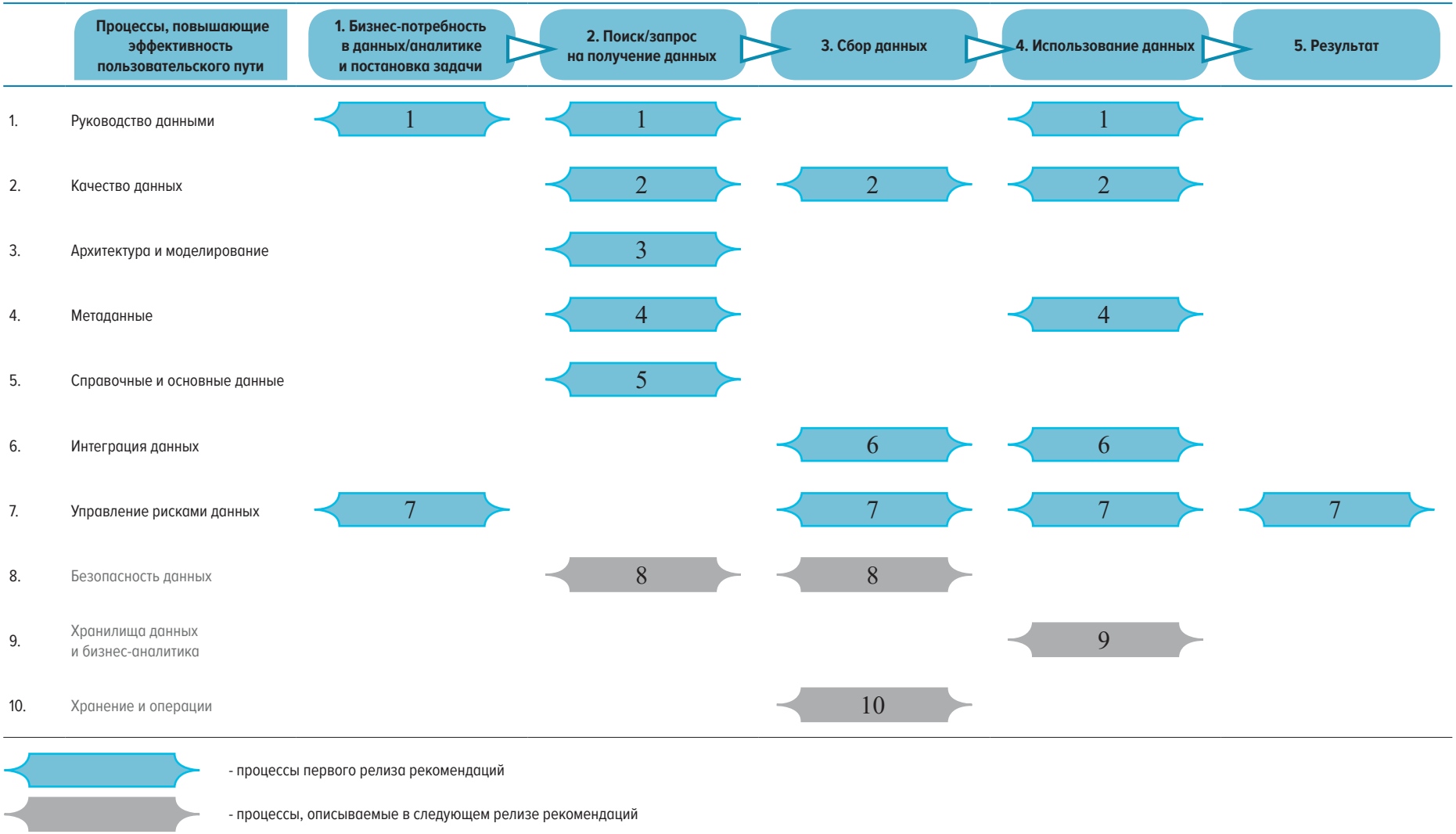
Ключевым процессом СУД является управление требованиями к данным. Когда количество аналитических запросов превышает определенный порог, становится целесообразным внедрение процессов системы управления требованиями. Это позволяет стандартизировать процесс формулирования задач, избежать дублирования и обеспечить контроль требований к данным.

Аналогично на этапе поиска данных критически важным становится использование результатов процесса управления метаданными. Если сотрудники тратят значительное время на поиск нужных данных, которые присутствуют в организации, то это сигнал к внедрению каталога данных и системы управления метаданными. Наличие каталога данных позволит пользователям сократить время на поиск нужных данных.

Для каждого процесса СУД можно сформулировать критерии, определяющие оправданность внедрения процесса. При срабатывании одного или нескольких таких критериев (табл. 2) целесообразно рассмотреть вопрос о развертывании соответствующих процессов.

При построении бизнес-кейсов можно использовать ряд драйверов, таких как сокращение времени на поиск и подготовку данных для аналитики, повышение точности аналитических выводов и прогнозов, снижение рисков, связанных с нарушением конфиденциальности данных, оптимизация затрат на хранение и обработку данных, улучшение соответствия регуляторным требованиям.

ПОЛЬЗОВАТЕЛЬСКИЙ ПУТЬ В РАБОТЕ С ДАННЫМИ СОТРУДНИКОВ УФР (USER JOURNEY MAP) *Рис. 1*



КРИТЕРИИ ОПРАВДАННОСТИ ВНЕДРЕНИЯ ПРОЦЕССОВ СУД

Табл. 2

Этап пользовательского пути	Название процесса	Базовые показатели для оценки. Критерий оправданности внедрения процесса
1. Бизнес-потребность в данных/аналитике и постановка задачи	**Руководство данными**	• Более 3 разнородных аналитических запросов/исследований в квартал, создающих необходимость создания новых дата-сервисов. • Более 5 тыс. стандартных запросов от федеральных органов исполнительной власти и (или) подобных обращений (например, по наследственным делам). • Более 5 учетных информационных систем и более 3 подразделений, требующих аналитику на основе данных из этих систем
2. Поиск/запрос на получение данных	**Руководство данными**	• Текущее значение интегральной самооценки зрелости СУД меньше **2** (из 5 возможных), и при этом организация ставит целью существенно увеличить зрелость. • Менее **40%** пользователей данных удовлетворены текущим качеством данных в организации
	Архитектура и моделирование данных	• Наличие более **20** сложных взаимосвязей между данными из разных систем[1]. • Акцентирована потребность создания единой модели данных для организации. • Организация создает новый аналитический контур или активно развивает существующий аналитический контур и бизнес-аналитику. • В организации отмечаются проблемы дублирования данных. • В организации существует несколько подходов к пониманию необходимости организации данных для аналитических задач. • Организация считает важным решить задачу получения единого мнения по критичным сущностям и показателям
	Качество данных	• Ежемесячно выявляется более **5** критических ошибок в показателях отчетности. • В среднем на исправление критических ошибок организации требуется более **5** рабочих дней. • Менее **40%** пользователей данных удовлетворены текущим качеством данных в организации
	Управление метаданными	• Акцентирована потребность в скорости поиска и понимания смысла, отслеживания статуса происхождения данных (Data Lineage), в первую очередь критичных. • Более **1 тыс.** уникальных полей данных используется в регулярной аналитике. • Аналитики организации тратят более **30%** времени на поиск и подготовку данных для выработки решений
	Справочные и основные данные	• Ключевые, регулярно обновляемые справочники распределены по **2 и более** информационным системам. • Акцентированы потребности организации: – в управлении данными о клиентах, продуктах и так далее; – в унификации справочников для задач B2B-интеграции
	Безопасность данных	• Присутствует потребность в классификации уровня доступа к данным. • Поставлена задача обеспечить полную прозрачность для проверки работы процедур доступа к данным. • Требуется выстроить процесс разработки или MLOps на обезличенных данных
3. Сбор данных	**Интеграция данных**	• Есть необходимость автоматизированной загрузки данных из более чем **5** разнородных источников. • Присутствует потребность в создании и развитии интеграции данных в режиме реального времени для более чем **5** ключевых бизнес-процессов. • Акцентирована важность единого представления данных о бизнес-сущности из разных систем (например, 360-градусный взгляд на клиента). • На интеграцию нового источника данных в среднем требуется более **20** человеко-дней
	Безопасность данных	• Ведется работа с персональными данными клиентов или финансовой информацией, требующей защиты. • Присутствует необходимость соответствия требованиям регуляторов по безопасности данных (например, GDPR, PCI DSS). • Возникла потребность в комплексной защите отдельных данных при передаче и хранении. • За последний год было зафиксировано более **3** инцидентов, связанных с утечкой данных. • Требуется выстроить процесс разработки или MLOps на обезличенных данных
	Хранение и операции с данными	• Объем хранимых данных превышает **10 Тб** или темп роста более **500 Гб** в месяц. • Необходимо обеспечить устойчивую оперативность получения данных по запросам (когда среднее время отклика должно составлять менее **1,5 с**)

[1] *Ситуации, когда одни данные зависят от других (в том числе данные из другой системы) или оказывают влияние на них. Пример: клиентские данные и данные по финансовым транзакциям, данные по оплатам счетов (когда есть специальные правила учета платежей по типам задолженности), зависимости между показателями разных учетных систем, работающих по разным алгоритмам учета.*

Этап пользовательского пути	Название процесса	Базовые показатели для оценки. Критерий оправданности внедрения процесса
	Качество данных	• Более **10%** критичных данных требуют очистки или обогащения перед использованием. • Акцентирована потребность организации в отслеживании статуса и качества собираемых данных, например при контроле соблюдения соглашения об уровне сервиса (OLA и/или SLA)[2] • Наличие требований от бизнес-процессов, результаты которых критически зависят от качества входных данных
4. Использование данных	**Качество данных**	• Аналитики организации при подготовке решений тратят более **30%** времени на подготовку и проверку данных для анализа в витринах данных. • Наличие ежемесячно более **5** регулярных инцидентов качества данных, которые могут повлечь существенные финансовые и/или репутационные риски, если они не будут своевременно обнаружены и устранены. • Акцентирована необходимость мониторинга качества данных для ключевых бизнес-процессов
	Хранилища данных и бизнес-аналитика	• Присутствует необходимость в регулярной отчетности более чем по **50** ключевым показателям эффективности. • Обозначена потребность в создании многомерных аналитических источников данных более чем для **5** важных задач анализа данных. • Бизнес-пользователями обоснована необходимость работы с self-service аналитикой более чем для **70%** регулярных отчетов
	Интеграция данных	• Выявлена потребность в создании единого аналитического слоя данных из разных источников. • Необходим автоматизированный обмен данными между приложениями
	Управление метаданными	• Акцентирована потребность в отслеживании происхождения и использования данных (Data Lineage) в **25** различных отчетах и/или аналитических моделях
	Руководство данными	• Принятие стратегических решений на основе аналитики происходит чаще чем раз в квартал • Текущее значение интегральной самооценки зрелости СУД меньше **2** (из 5 возможных), при этом организация ставит цель существенно увеличить зрелость
5. Результат	**Управление рисками и соблюдение нормативных требований к данным**	• Ежегодные финансовые потери из-за низкого качества данных составляют более **3 млн руб.**, и таких событий более 3. • Организация считает, что риски финансовых потерь или применения регуляторных санкций существенны и вероятность их наступления велика. • Менее **30%** критических бизнес-процессов покрыто проверками качества данных

[2] Соглашения между заказчиком и исполнителем о качестве оказываемых услуг. В соглашении описываются параметры предоставления услуг: качество, количество, сроки, момент предоставления, время реакции и другие важные для заказчика параметры.
***Operational Level Agreement (OLA)** – внутреннее соглашение в организации, определяющее зоны ответственности и параметры предоставления услуг между подразделениями.*
***Service Level Agreement (SLA)** – договор между заказчиком и поставщиком, содержащий описание услуги, права, обязанности сторон и штрафные санкции за нарушение условий предоставления услуг.*

Если один или несколько описанных выше критериев оправданности внедрения процессов выполняются в один или несколько этапов пользовательского пути / этапов процесса, то можно ставить вопрос о развертывании процессов СУД.

Внедрение процессов СУД в деятельность организации способно трансформировать практику и культуру работы процессов организации, поэтому важно предусматривать поэтапный план внедрения, в котором каждый этап должен иметь самостоятельную ценность для организации.

При таком подходе СУД может стать полезным инструментом повышения эффективности и конкурентоспособности организации.

3. КОНЦЕПТУАЛЬНЫЙ ДИЗАЙН ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ»

Описание концептуального дизайна процесса «Управление рисками данных» происходит с помощью описанной выше **карточки процесса**.

Карточка процесса включает:

1. Цели процесса «Управление рисками данных».
2. Участники процесса «Управление рисками данных».
3. Объекты процесса «Управление рисками данных».
4. Требования к процессу «Управление рисками данных».
5. Методы, обеспечивающие процесс «Управление рисками данных».
6. Показатели эффективности процесса «Управление рисками данных».

Описание организации эффективного процесса «Управление рисками данных» дополняется сводной таблицей организации процесса «Управление рисками данных», описанием типовых проблем и способов их решения.

Завершается описание концептуального дизайна описанием организации зон ответственности в процессе в виде матрицы RACI.

3.1. Карточка концептуального дизайна процесса «Управление рисками данных»

3.1.1. Цели процесса «Управление рисками данных»

1. Определение причин возникновения инцидентов качества данных.
2. Выявление системных причин повторяющихся инцидентов качества данных для корректировки процессов.
3. Обеспечение соответствия процессов организации, использующих критичные данные, нормативным требованиям работы с данными (Приложение 3).

3.1.2. Участники процесса «Управление рисками данных»[1]

Для успешной реализации бизнес-процессов организации важно вовлечение и слаженное взаимодействие различных подразделений и специалистов организации в работу со справочными данными организации.

Рекомендованными участниками процесса «Управление рисками данных» в организации являются:

1. Уполномоченный коллегиальный орган по управлению данными[2].
2. Директор по управлению данными / Директор по данным.
3. Офис директора по данным.
4. Владелец данных.

---

[1] Кредитные организации (головные кредитные организации банковской группы) обеспечивают реализацию требований к участникам процесса управления операционным риском в соответствии с требованиями Положения Банка России № 716-П.

[2] Допускается изменение в соответствии с принятыми в организации практиками управления рисками. В роли коллегиального органа по управлению рисками данных может выступать иной коллегиальный орган, на котором решаются вопросы по управлению рисками, важно, чтобы в работу данного коллегиального органа был вовлечен Директор по данным.

5. Офицер данных.
6. Потребитель данных.

Описание ролей приведено в Приложении 5.

Эффективное управление рисками данных рекомендуется встраивать в общую систему корпоративного управления рисками организации. Помимо ролей, установленных в рамках системы управления данными, в процесс управления рисками данных целесообразно вовлекать **Службу управления рисками.**

Руководитель Службы управления рисками[3] обеспечивает интеграцию рисков данных в корпоративную систему управления рисками. В его зону ответственности входит разработка единых стандартов их оценки, комплексная оценка влияния рисков данных на деятельность организации и контроль риск-аппетита.

Взаимодействие Директора по управлению данными и Руководителя службы управления рисками рекомендуется выстраивать на регулярной основе с закреплением порядка обмена информацией. Конкретные формы взаимодействия определяются организацией самостоятельно с учетом масштаба деятельности и организационной структуры.

3.1.3. Объекты процесса «Управление рисками данных»

Объектами управления является совокупность следующих объектов управления (табл. 3):
1. Профиль риска данных.
2. Событие риска данных.
3. Риск данных.
4. Ключевые индикаторы риска данным (КИРД).
5. Мероприятия по снижению риска данных.

ОБЪЕКТЫ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 3*

№	Название объекта	Описание объекта
1	**Профиль риска данных**	Структурированная совокупность выявленного риска данных. Включает классификацию рисков по источникам возникновения (технологические, процессные, человеческие факторы), областям воздействия и критичности для бизнес-процессов. Содержит ссылки на соответствующие идентификаторы рисков из реестра операционных рисков (в целях информационной привязки, без передачи функций управления)
2	**Событие риска данных**	Событие операционного риска, реализация которого связана с инцидентом качества данных. Пример карточки события риска данных приведен в Приложении 6
3	**Риск данных**	Вероятность изменения свойств или характеристик качества данных, которые могут привести к прямым или непрямым потерям. Риск данных является подвидом риска информационных систем. Пример карточки риска данных приведен в Приложении 7
4	**Ключевые индикаторы риска данных (КИРД)**	Опережающие метрики для мониторинга накопления факторов риска до их материализации

[3] В соответствии с Указанием Банка России от 25.12.2017 № 4662-У «О квалификационных требованиях к руководителю службы управления рисками, службы внутреннего контроля и службы внутреннего аудита кредитной организации, лицу, ответственному за организацию системы управления рисками, и контролеру негосударственного пенсионного фонда, ревизору страховой организации, о порядке уведомления Банка России о назначении на должность (об освобождении от должности) указанных лиц (за исключением контролера негосударственного пенсионного фонда), специальных должностных лиц, ответственных за реализацию правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма кредитной организации, негосударственного пенсионного фонда, страховой организации, управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, микрофинансовой компании, сотрудника службы внутреннего контроля управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, а также о порядке оценки Банком России соответствия указанных лиц (за исключением контролера негосударственного пенсионного фонда) квалификационным требованиям и требованиям к деловой репутации».

№	Название объекта	Описание объекта
5	**Мероприятия по снижению риска данных**	Комплексная совокупность организационных, методологических и технологических инициатив, направленных на систематическое улучшение способности организации выявлять и предотвращать реализацию рисков данных. Мероприятия включает: 1. Стратегические инициативы – масштабные изменения в архитектуре данных, модернизация платформ, внедрение новых технологий управления качеством. 2. Процессные улучшения – оптимизация процессов создания, обработки и использования данных, внедрение лучших практик управления данными. 3. Развитие компетенций – повышение уровня грамотности персонала, формирование культуры ответственного обращения с данными. 4. Технологические меры – внедрение технологических средств автоматизации мониторинга качества данных, инструментов профилирования и очистки данных. 5. Мониторинг качества данных – регулярная оценка значений показателей качества и их сопоставление с целевыми уровнями. 6. Реагирование на нарушения качества данных – выполнение комплекса мероприятий при выходе показателей за предельно допустимые значения: информирование ответственных лиц, анализ первопричин нарушения качества данных, корректировка данных (очистка / обогащение / исправление ошибок), при необходимости – пересмотр бизнес-процессов, использующих данные

Целесообразно дать разграничения между объектами управления: мероприятиями по снижению риска данных, ключевыми индикаторами риска данных и событиями риска данных (рис. 2).

Предполагается, что перед началом мониторинга Владельцы данных и Потребители данных определяют требования к характеристикам качества данных. И далее Владелец данных совместно с Директором по управлению данными и Руководителем СУР определяют состав КИРД и их пороговые значения.

На рис. 2 представлен механизм выявления, фиксации и системного реагирования на события риска данных, являющиеся потенциальными в отношении признания их операционными рисками, связанными с обработкой данных. Идентификация риска данных для кредитных организаций (головных кредитных организаций банковской группы) осуществляется в рамках системы управления операционными рисками в соответствии с требованиями Положения Банка России № 716-П.

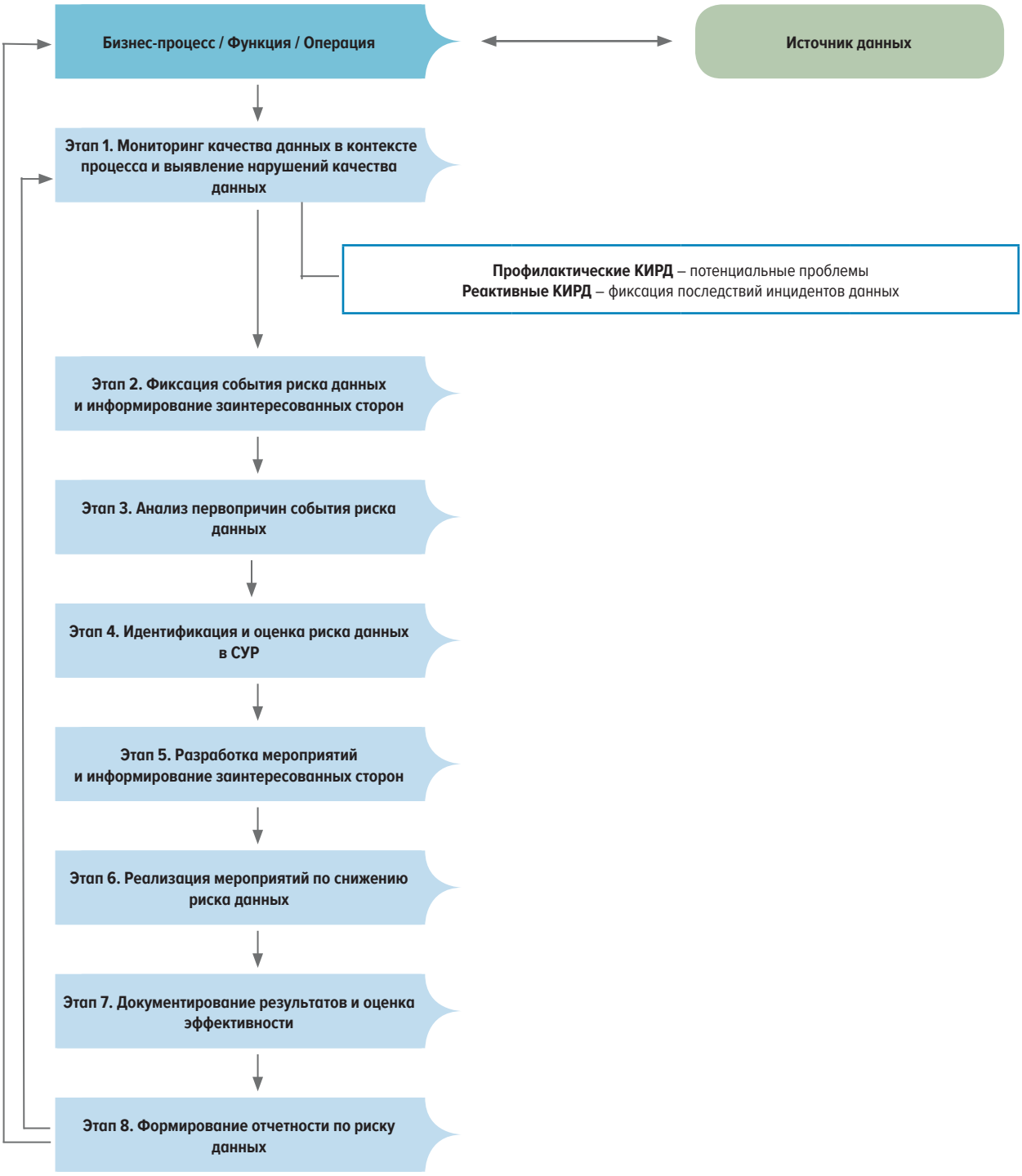
Этап 1. Процесс инициируется при выполнении бизнес-процесса или операции, в ходе чего производится мониторинг КИРД. Автоматизированные и ручные контроли обеспечивают выявление отклонений от установленных требований к характеристикам данных.

На *этапе 2* при выявлении несоответствия фиксируются несоответствие данных установленным требованиям в виде инцидента качества данных. Производится первичная оценка инцидента качества данных и по результатам проверки условий регистрации события риска данных может быть создано событие риска данных. Событие риска данных регистрируется в базе событий операционного риска и становится доступно СУР.

Выполняется анализ корневых причин события риска данных с применением методологии, утвержденной внутренними документами кредитной организации *(этап 3)*. Анализ проводится в целях установления системных факторов возникновения события риска данных и определения области распространения риска.

По результатам анализа корневых причин осуществляется процедура идентификации и оценки риска данных *(этап 4)* в порядке, установленном внутренними документами по управлению операционным риском. В рамках взаимодействия с СУР устанавливается связь события риска данных с существующими рисками в корпоративном реестре операционных рисков. При отсутствии соответствующего риска инициируется процедура добавления нового риска силами подразделения по управлению операционными рисками. Оценка риска данных производится в соответствии с методикой, обеспечивающей сопоставимость оценок различных видов риска данных.

ВЗАИМОСВЯЗЬ МЕЖДУ ОБЪЕКТАМИ УПРАВЛЕНИЯ *Рис. 2*



На основании результатов идентификации и оценки риска формируется план мероприятий по минимизации риска данных с вовлечением владельцев данных, владельцев процессов и иных заинтересованных сторон *(этап 5)*. Утверждается комплекс мероприятий с распределением ответственности и сроков исполнения.

На *этапе 6* реализуются мероприятия по снижению риска данных 2 типов:
1. *оперативные (корректирующие)* – устранение последствий произошедшего инцидента качества данных и восстановление качества данных;
2. *превентивные (предупреждающие)* – организационные, технологические и методологические инициативы, направленные на предотвращение повторения подобных инцидентов качества данных.

На *этапе 7* осуществляется верификация эффективности проведенных мероприятий через анализ динамики КИРД и частоты однотипных событий риска данных. Результаты оценки фиксируются в реестре операционных рисков СУР.

По итогам выполнения на *этапе 8* формируется отчет, содержащий описание события, анализ первопричин, результаты оценки эффективности мероприятий и извлеченные уроки. Отчет используется для совершенствования процессов обработки данных и актуализации внутренних документов по управлению операционным риском.

3.1.4. Требования к процессу «Управление рисками данных»

Управление рисками данных требует системного подхода и разграничения ответственности между участниками процесса.

В целях обеспечения эффективности работы процесса «Управление рисками данных» рекомендуется рассмотреть следующие требования к организации процесса:
1. Систематическое выявление рисков данных.
2. Регистрация и анализ событий риска данных.
3. Обеспечение полноты классификации рисков данных.
4. Обеспечение функциональной полноты управления риском данных.
5. Мониторинг ключевых индикаторов риска данных.

Содержание требований представлено в табл. 4. Данные требования целесообразнее всего реализовывать при непосредственной координации Директора по данным и/или Офиса директора по данным.

ТРЕБОВАНИЯ К ПРОЦЕССУ «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 4*

№	Требование	Описание требования
1	**Систематическое выявление рисков данных**	Процесс идентификации факторов, способных привести к реализации потерь вследствие изменения свойств или характеристик качества данных
2	**Регистрация и анализ событий риска данных**	Должно обеспечиваться систематическое документирование, проведение количественной и качественной оценки нарушений/инцидентов качества данных, включая технические сбои, ошибки персонала, с последующим анализом причин, оценкой воздействия и документированием принятых мер по устранению и предотвращению повторных случаев. Так, например, оценка может быть: • количественной (прямые убытки, штрафы, упущенная выгода) • качественной (например, на основе данных о потерях от данного риска в других организациях)
3	**Обеспечение полноты классификации рисков данных**	Метод предусматривает формирование организацией Классификатора типовых событий риска данных по признакам*: источники и причины возникновения нарушения характеристик качества данных
4	**Обеспечение функциональной полноты управления риском данных**	Система включает процедуры выявления и оценки рисков данных, классификаторы событий риска данных, базы инцидентов качества данных, определенные ответственные подразделения, автоматизированные системы и механизмы координации между структурными подразделениями для эффективного управления операционными рисками
5	**Мониторинг ключевых индикаторов риска данных**	Разработка и регулярная оценка индикаторов риска данных, сигнализирующих о возможном повышении уровня риска данных. Устанавливаются пороговые значения и определяются процедуры информирования заинтересованных сторон при их превышении для своевременного реагирования

** Приложение 2 к Положению Банка России от 02.11.2024 № 845-П «О порядке расчета величины кредитного риска банками с применением банковских методик управления кредитным риском и моделей количественной оценки кредитного риска».*

3.1.5. Методы, обеспечивающие процесс «Управление рисками данных»

Описанные ниже методы призваны обеспечить реализацию представленных выше требований к процессу:

1. Разработка онтологии рисков данных.
2. Сопровождение и развитие КИРД.
3. Информирование заинтересованных сторон о наступлении событий риска данных.
4. Самооценка управления риском данных.
5. Сводная отчетность по рискам.
6. Проведение самооценки подверженности рискам данных.
7. Регистрация и анализ корневых причин событий риска данных.

Содержание методов, обеспечивающих процесс, раскрыто в табл. 5.

МЕТОДЫ, ОБЕСПЕЧИВАЮЩИЕ ПРОЦЕСС «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 5*

№	Метод	Описание метода
1	**Разработка онтологии рисков данных***	Построение понятийной модели, систематизирующей явления, связанные с дефектами данных, через определение категорий, атрибутов, причинно-следственных связей и типовых сценариев возникновения проблем. Онтология обеспечивает единое понимание терминов и классификации среди подразделений, участвующих в обработке данных. На основе онтологии формируется Классификатор типовых событий риска данных, анализа повторяющихся паттернов инцидентов качества данных и подготовки отчетности
2	**Сопровождение и развитие КИРД**	Регулярное обновление состава, порогов и алгоритмов ключевых индикаторов риска данных с учетом изменений в бизнес-процессах, системах и регуляторных требованиях
3	**Информирование заинтересованных сторон о наступлении событий риска данных**	Регламентированная процедура, посредством которой владельцы процессов и/или данных уведомляют подразделение по управлению операционными рисками и иные заинтересованные стороны о выявленном событии риска данных с предоставлением полного набора сведений (описание, атрибуты, КИРД, последствия, первопричины)
4	**Самооценка управления риском данных**	Процедуры самооценки в управлении риском данных включают 4 самостоятельных вида самооценки: 1) самооценку риска данных – выявление и оценку уровня риска данных в процессах и информационных системах; 2) самооценку соответствия нормативным требованиям к данным – превентивную проверку выполнения обязательных требований, связанных с качеством, полнотой и достоверностью данных, используемых в регламентированной деятельности; 3) самооценку уровня зрелости управления данными – оценку развитости системы управления данными по установленной шкале; 4) оценку эффективности управления риском данных – анализ динамики показателей и результативности принятых мер. Процедуры самооценки организуются Владельцами процессов и Владельцами данных на основе контрольных вопросов, формализованных критериев и выборочного анализа
5	**Сводная отчетность по рискам данных**	Регулярно формируемые отчеты**, обобщающие результаты управления операционным риском в части, относящейся к качеству данных. Отчеты обобщают сведения 2 сегментов: – качество данных – отражает результаты мониторинга соблюдения установленных требований к качеству данных, эффективность проведенных корректирующих и предупреждающих мероприятий, а также иную информацию, формируемую в рамках внутренних процедур управления данными; – риск данных – содержит детализированные сведения о реализовавшихся событиях риска данных и динамике КИРД. Отчетность предназначена для информирования руководства, органов управления данными и подразделения по управлению рисками о состоянии операционного риска в части данных и результатах работы по его минимизации
6	**Проведение самооценки подверженности рискам данных**	Периодическая процедура внутренней диагностики, обеспечивающая вовлечение бизнес-подразделений в проактивное выявление потенциальных рисков данных посредством структурированных опросников, чек-листов и сценарного анализа, позволяющая сформировать децентрализованную карту рисков данных и повысить риск-культуру организации
7	**Регистрация и анализ корневых причин событий риска данных**	Двухэтапная процедура: 1) документирование событий риска данных в реестре с фиксацией времени, систем, объемов и последствий; 2) проведение анализа корневых причин методами RCA для выявления первопричин – системных, процессных или технических факторов, приведших к событию риска данных

* Онтология рисков данных – это концептуальная модель предметной области «Риски данных», представляющая собой структурированное описание всех типов рисков, их атрибутов, взаимосвязей и правил, обеспечивающая единое понимание и системный подход к идентификации, классификации и управлению рисками данных в организации. Онтология применяется при идентификации рисков, для контроля полноты анализа процессов, анализе взаимосвязей для выявления каскадных эффектов в рисках данных, приоритизации, в процессах отчетности для агрегации рисков.

*** Для кредитных организаций (головных кредитных организаций банковской группы) требования к составлению отчетности в рамках системы управления операционным риском установлены Положением Банка России № 716-П.*

3.1.6. Показатели эффективности процесса «Управление рисками данных»

Для организаций с уровнями зрелости процесса «Управление рисками данных»: «Начальный уровень», «Уровень осознания», «Уровень применения» рекомендованы следующие показатели:

1. Динамика потерь по событиям риска данных (%).
2. Доля бизнес-процессов, покрытых КИРД (%).
3. Доля идентифицированных рисков данных, обеспеченных планами мероприятий по снижению риска данных (%).
4. Доля событий риска данных, связанных с ранее идентифицированными рисками данных (%).

Описание показателей приведено в табл. 6.

ПОКАЗАТЕЛИ, ОБЕСПЕЧИВАЮЩИЕ ПРОЦЕСС «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 6*

№	Показатель	Назначение показателя	Описание показателя
1	**Динамика потерь по событиям риска данных (%)**	Показывает динамику изменений совокупных потерь по риску данных. Рост потерь по риску данных сигнализирует об ухудшении ситуации	Динамика (%) = (A – B) / B × 100%, где: • A – совокупные потери по событиям риска данных за отчетный месяц; • B – совокупные потери по событиям риска данных за предшествующий отчетному месяц*. Периодичность: ежемесячно. Источник: Реестр операционных рисков
2	**Доля бизнес-процессов, покрытых ключевыми индикаторами риска данных (КИРД)**	Оценивает охват процесса управления рисками данных мониторингом КИРД и показывает, насколько уровень риска данных контролируется в процессе «Управление рисками данных»	Доля (%) = A / B × 100%, где: • A – число ключевых бизнес-процессов с действующими КИРД (организация самостоятельно определяет методологию, сколько КИРД должно работать по ключевому бизнес-процессу); • B – общее число ключевых бизнес-процессов. Периодичность: раз в полгода. Источники: Реестр операционных рисков, Реестр КИРД
3	**Доля идентифицированных рисков данных, обеспеченных планами мероприятий по снижению риска данных**	Отражает полноту охвата выявленных рисков данных превентивными мерами и характеризует проактивность системы управления рисками данных	Доля (%) = A / B × 100%, где: • A – количество идентифицированных рисков данных с утвержденными планами мероприятий по снижению риска; • B – общее количество идентифицированных рисков данных, требующих снижения согласно риск-аппетиту организации. Периодичность: ежеквартально. Источники: Реестр рисков данных, Реестр мероприятий по минимизации рисков
4	**Доля событий риска данных, связанных с ранее идентифицированными рисками данных (%)**	Оценивает полноту и актуальность процесса идентификации рисков данных, а также эффективность превентивных мер по управлению известными рисками. Низкое значение 0–40% может свидетельствовать о пробелах в идентификации рисков и появления новых, ранее не учтенных угроз	Доля (%) = A / B × 100%, где: • A – число событий риска данных, для которых установлена связь с ранее включенными в реестр рисков данных; • B – общее число зарегистрированных событий риска данных за период. Периодичность: ежеквартально. Источники: Реестр событий риска данных, Реестр операционных рисков с датами первичной идентификации

* Если совокупные потери за предшествующий месяц равны нулю (B = 0), расчет динамики (%) по стандартной формуле не производится. Вместо этого показатель анализируется в связке с абсолютным значением совокупных потерь за отчетный месяц (A). При A = 0 – динамика считается нулевой (отсутствие риска); при A > 0 – фиксируется как новое событие риска, и его значимость оценивается по величине A в контексте пороговых значений или исторических аналогов.

Комментарии к показателям:

1. Организация самостоятельно определяет алгоритмы и источники информации для расчета показателей.
2. Критерии информирования заинтересованных сторон при достижении КИРД пороговых значений подлежат пересмотру не реже одного раза в год на основе накопленной статистики инцидентов качества данных.

3. Основными источниками данных для расчета показателей являются системы регистрации и управления инцидентами организации, а также база событий операционного риска. Дополнительно используются результаты расчета КИРД, данные систем мониторинга рисков и результаты проверок качества данных.

3.2. Организация эффективного процесса «Управление рисками данных» и типовые проблемы

3.2.1. Организация эффективного процесса «Управление рисками данных»

Описание процесса «Управление рисками данных» приведено в Приложении 8. «Организация процесса «Управление рисками данных» должна начинаться с разработки методологии по управлению риском данных».

В табл. 7 представлено соотнесение требований к процессу «Управление рисками данных» с обеспечивающими его методами, а также рекомендации по показателям оценки эффективности.

СВОДНАЯ ТАБЛИЦА ОРГАНИЗАЦИИ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 7*

№	Требования к процессу, см. пункт 3.1.4	Методы, обеспечивающие процесс, см. пункт 3.1.5
1	**Систематическое выявление рисков данных**	• Сопровождение и развитие КИРД • Проведение самооценки подверженности рискам данных
2	**Регистрация и анализ событий риска данных**	• Информирование заинтересованных сторон о наступлении событий риска данных • Регистрация и анализ корневых причин событий риска данных
3	**Обеспечение полноты классификации рисков данных**	• Разработка онтологии рисков данных
4	**Обеспечение функциональной полноты управления риском данных**	• Самооценка управления риском данных • Сводная отчетность по рискам данных • Информирование заинтересованных сторон о наступлении событий риска данных • Проведение самооценки подверженности рискам данных
5	**Мониторинг ключевых индикаторов риска данных (КИРД)**	• Сопровождение и развитие КИРД • Определение критериев существенности для событий риска данных • Сводная отчетность по рискам данных

3.2.2. Типовые проблемы и подходы к их решению

В Приложении 9 к настоящему документу «Типовые проблемы и подходы к их решению» описаны типовые проблемы процесса «Управление рисками данных» и примеры подходов к их возможному решению.

Выбор подхода к решению управленческих ситуаций зависит от большого числа факторов, включая особенности корпоративной культуры в подготовке и принятии решений. Поэтому целью описанных подходов является не следование им, а нахождение пути наименьшего сопротивления внедрения процессов управления данными.

3.3. Концептуальное содержание процесса «Управление рисками данных»

Концептуально процесс «Управление рисками данных» предваряется работой Владельцев бизнес-процессов по оценке критичности данных на основе оценки критичности бизнес-процессов и их функций и состоит из совокупности следующих блоков:

1. Разработка методологии управления рисками данных.

1.1. Разработка/совершенствование методологии соотнесения рисков данных с СУР организации.
1.2. Описание/актуализация процесса управления рисками данных.
1.3. Определение и настройка КИРД, установка пороговых значений и правил информирования.
1.4. Идентификация и регистрация рисков данных в СУР.

2. Выявление и регистрация событий риска данных.

2.1. Выявление среди инцидентов качества данных потенциальных событий риска данных (из ИТ-систем или других источников).
2.2. Анализ инцидентов качества данных и их типизация по степени влияния на бизнес-процессы.
2.3. Предварительная оценка последствий события риска данных.
2.4. Фиксация событий риска данных.

3. Обследование событий риска данных и определение источников риска.

3.1. Анализ корневых причин (RCA) событий риска данных.
3.2. Оценка влияния и приоритизация инцидентов качества данных на смежные процессы и ИТ-системы.
3.3. Самооценка рисков данных.
3.4. Документирование результатов исследований и регистрация выявленных рисков данных.

4. Разработка и реализация планов мероприятий по снижению риска данных.

4.1. Координация исправления данных и причин инцидентов качества данных.
4.2. Формирование проектов/инициатив по совершенствованию процессов обработки данных и повышению качества данных.
4.3. Координация выполнения проектов/инициатив с владельцами данных и процессов.
4.4. Анализ и оценка эффективности КИРД и мероприятий по рискам данных.

5. Мониторинг риск-отчетности и информирование.

5.1. Подготовка сведений для включения в отчетность по СУР.
5.2. Информирование коллегиальных органов управления и заинтересованных сторон о рисках данных.
5.3. Пополнение базы знаний по событиям риска данных.

3.4. Зоны ответственности в процессе «Управление рисками данных» (матрица RACI)

В табл. 8 описаны рекомендации по зонам ответственности и выходным артефактам процесса «Управление рисками данных» (матрица RACI).

ЗОНЫ ОТВЕТСТВЕННОСТИ В ПРОЦЕССЕ «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» (МАТРИЦА RACI) *Табл. 8*

Процесс/подпроцесс		Коллегиальный орган по УД	Директор по данным	Офис Директора по данным	Владельцы данных	Офицер данных	Потребитель данных	Выходные артефакты
(1)		(2)	(3)	(4)	(5)	(6)	(7)	(8)
1. Разработка методологии управления рисками данных								
1.1	Разработка/совершенствование методологии соотнесения рисков данных с СУР организации	I	R/A*	R	R	R	I	D064 Регламент процесса управления рисками в области данных; D166 Реестр ответственных за риски данных; D174 Классификатор типовых событий рисков данных
1.2	Описание/актуализация процесса управления рисками данных	I	R/A*	R	R	R	C	D064 Регламент процесса управления рисками в области данных; D170 Запросы на изменения КИРД по рискам данных
1.3	Определение и настройка КИРД, установка пороговых значений и правил информирования	I	C	R/A*	R	R	R	D160 Реестр ключевых индикаторов риска данных (КИРД); D170 Запросы на изменения КИРД по рискам данных
1.4	Идентификация и регистрация рисков данных в СУР	I	I	C	R/A*	R	C	D173 Карточка риска данных; D174 Классификатор типовых событий рисков данных
2. Выявление и регистрация событий риска данных								
2.1	Выявление среди инцидентов качества данных потенциальных событий риска данных (из ИТ-систем или других источников)	I	I	C	A	R	R	D168 Отчет о срабатывании проверок качества данных и алерты по превышению пороговых значений; D074 Реестр проблем (управление данными); D173 Карточка риска данных
2.2	Анализ инцидентов качества данных и их типизация по степени влияния на бизнес-процессы	I	I	C	A	R	C	D158 Карточка события риска данных;
2.3	Предварительная оценка последствий события	I	C	C	A	R	C	D158 Карточка события риска данных
2.4	Фиксация событий риска данных	I	I	C	A	R	I	D158 Карточка события риска данных; D173 Карточка риска данных
3. Обследование событий риска данных и определение источников риска								
3.1	Анализ корневых причин (RCA) событий риска данных	I	C	C	R	R/A*	R	D159 Отчеты RCA по событиям риска данных; D173 Карточка риска данных
3.2	Оценка влияния и приоритизация инцидентов качества данных на смежные процессы и ИТ-системы	I	C	A	R	R	R	D159 Отчеты RCA по событиям риска данных; D044 Отчет о рисках, связанных с низким качеством данных; D173 Карточка риска данных
3.3	Самооценка рисков данных	I	I	C	A	R	C	D044 Отчет о рисках, связанных с низким качеством данных; D173 Карточка риска данных
3.4	Документирование результатов исследований и регистрация выявленных рисков данных	I	R/A*	R	R	R	I	D159 Отчеты RCA по событиям риска данных; D173 Карточка риска данных
4. Разработка и реализация планов мероприятий по снижению риска данных								
4.1	Координация исправления данных и причин инцидентов качества данных	I	C	C	A	R	C	D074 Реестр проблем (управление данными); D167 Отчет о статусе планов устранения проблем качества данных; D173 Карточка риска данных

	Процесс/подпроцесс	Коллегиальный орган по УД	Директор по данным	Офис Директора по данным	Владельцы данных	Офицер данных	Потребитель данных	Выходные артефакты
4.2	Формирование проектов/ инициатив по совершенствованию процессов обработки данных и повышению качества данных	A	C	R	R	C	I	D101 Стратегия и план развития СУД в части минимизации рисков данных; D074 Реестр проблем (управление данными)
4.3	Координация выполнения проектов/инициатив с владельцами данных и процессов	I	C	C	R	C	I	D167 Отчет о статусе планов устранения проблем качества данных; D173 Карточка риска данных
4.4	Анализ и оценка эффективности КИРД и мероприятий по рискам данных	I	R/A*	R	R/C	C	I	D047 Отчет по эффективности мер повышения качества данных; D161 Отчет об эффективности КИРД; D173 Карточка риска данных
5. Мониторинг риск-отчетности и информирование								
5.1	Подготовка сведений для включения в отчетность по СУР	C	C	R/C	A/R	R	I	D165 Отчетность и информационные панели по рискам данных; D043 Отчет о проблемах качества данных, требующих внимания руководства; D173 Карточка риска данных
5.2	Информирование коллегиальных органов управления и заинтересованных сторон о рисках данных	A	R	R	R	I	I	D165 Отчетность и информационные панели по рискам данных; D043 Отчет о проблемах качества данных, требующих внимания руководства
5.3	Пополнение базы знаний по событиям риска данных	I	R/A*	R	R	R	I	D169 База знаний по управлению рисками данных; D174 Классификатор типовых событий рисков данных

** Определяется исходя из раздела 1.2 Модель процесса «Управление рисками данных», подраздел «Распределение ответственности между СУД и СУР».*

Организациям, исходя из выбранной стратегии развития системы управления данными, рекомендуется самостоятельно определять состав необходимых артефактов (табл. 9):

РЕКОМЕНДАЦИИ ПО СОСТАВУ АРТЕФАКТОВ ПО УРОВНЯМ ЗРЕЛОСТИ ДЛЯ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 9*

Код	Название артефакта	Минимальный состав артефактов по уровням зрелости		
		Начальный уровень и уровень осознания	Уровень применения	Уровень операционализации и трансформации
D044	**Отчет о рисках, связанных с низким качеством данных**			1
D064	**Регламент процесса управления рисками в области данных**			1
D158	**Карточка события риска данных**		1	1
D159	**Отчеты RCA по событиям риска данных**			1
D160	**Реестр КИРД**			1
D161	**Отчет об эффективности КИРД**			1
D165	**Отчетность и информационных панелей по рискам данных**		1	1
D166	**Реестр ответственных за риски данных**	1	1	1
D169	**База знаний по управлению рисками данных**			1
D170	**Запросы на изменения КИРД по рискам данных**		1	1
D173	**Карточка риска данных**		1	1
D174	**Классификатор типовых событий рисков данных**		1	1

3.5. Типовые артефакты процесса «Управление рисками данных»

В табл. 10 представлены типовые артефакты процесса «Управление рисками данных».

ТИПОВЫЕ АРТЕФАКТЫ ПРОЦЕССА «УПРАВЛЕНИЕ РИСКАМИ ДАННЫХ» *Табл. 10*

Код	Артефакт	Описание содержания
D044	**Отчет о рисках, связанных с низким качеством данных**	Комплексный отчет о рисках, связанных с низким качеством данных. Включает описание рисков, их оценку (вероятность и потенциальный ущерб), анализ причин возникновения. Обязательные элементы: категоризация рисков, связь с бизнес-процессами, оценка финансового и репутационного влияния, меры по устранению проблем качества данных, мониторинг эффективности мер, сценарии реализации рисков
D064	**Регламент процесса управления рисками в области данных**	Регламент процесса управления рисками в области данных содержит методологию выявления на основе инцидентов качества данных, оценку вероятности и воздействия рисков данных, матрицу рисков данных, стратегии реагирования на риски, процедуры мониторинга и отчетности, роли и ответственности, периодичность пересмотра рисков
D158	**Карточка события риска данных**	Формализованная запись, фиксирующая факт реализации риска данных и содержащая набор обязательных и опциональных атрибутов, описывающих событие, его причины, классификацию и связанный с событием инцидент качества данных. Предназначена для регистрации и анализа в рамках системы управления данными организации (Приложение 6)
D159	**Отчеты RCA по событиям риска данных**	Аналитический документ, содержащий результаты исследования корневых причин реализовавшихся событий риска данных. Включает хронологию развития событий риска данных, диаграммы причинно-следственных связей, выявленные системные и организационные факторы, способствовавшие реализации риска. Документирует цепочки отказов проверок качества данных, человеческие ошибки, технологические сбои и процессные недостатки. Содержит рекомендации по предотвращению повторения аналогичных событий риска данных, требования к совершенствованию и предложения по изменению процессов обработки данных
D160	**Реестр КИРД**	Каталог показателей раннего предупреждения о потенциальной реализации рисков данных, содержащий спецификации индикаторов, формулы расчета, источники данных, пороговые значения и правила эскалации. Для каждого КИРД определены связь с конкретными рисками, периодичность измерения, ответственные за мониторинг, история изменений пороговых значений. Включает классификацию индикаторов по типам (опережающие, текущие, запаздывающие), критичности и доменам данных. Обеспечивает основу для автоматизированного мониторинга состояния рисков и своевременного реагирования
D161	**Отчет об эффективности КИРД**	Документ, оценивающий результативность системы КИРД в предотвращении и выявлении рисков данных. Содержит статистику срабатываний КИРД, анализ их предиктивной способности, процент предотвращенных инцидентов качества данных, оценку ложных срабатываний. Включает сравнение фактических событий риска данных с прогнозами КИРД, анализ пропущенных нарушений проверками качества данных, рекомендации по оптимизации пороговых значений
D165	**Отчетность и информационные панели по событиям рискам данных**	Интегрированная система визуализации текущего состояния рисков данных организации, предоставляющая руководству оперативную информацию через интерактивные дашборды и регулярные отчеты. Включает тепловые карты рисков, тренды событий риска данных, статус, КИРД. Обеспечивает детализацию возможности перехода от агрегированных метрик к детальным сведениям по рискам данным
D166	**Реестр ответственных за риски данных**	Документ, закрепляющий персональную ответственность за управление конкретными рисками данных в организации. Содержит сопоставление рисков с владельцами данных или процессов, указание зон ответственности, контактную информацию, заместителей, сроки пересмотра назначений. Включает матрицу эскалации для различных уровней критичности событий, определение полномочий по принятию решений о приемлемости рисков
D169	**База знаний по управлению рисками данных**	Структурированное хранилище накопленного опыта, лучших практик, извлеченных уроков и методических материалов по управлению рисками данных. Содержит каталог типовых рисков с описанием сценариев реализации, Реестр проверок качества данных, шаблоны документов, чек-листы, примеры успешных кейсов. Включает раздел FAQ, глоссарий, ссылки на нормативные требования и другие материалы, которые пригодны для обучения сотрудников
D170	**Запросы на изменения КИРД по рискам данных**	Формализованные запросы на модификацию существующих или внедрение новых КИРД. Содержат обоснование необходимости изменений, описание предлагаемых модификаций, оценку влияния на процессы и требуемые ресурсы. Включают результаты анализа эффективности текущих мер, бизнес-кейс для изменений, план внедрения, критерии успеха
D173	**Карточка риска данных**	Формализованная запись, содержащая набор обязательных и опциональных атрибутов для идентификации, классификации и оценки риска данных. Применяется для учета и контроля в системе управления операционными рисками организации (Приложение 7)
D174	**Классификатор типовых событий рисков данных**	Справочник, систематизирующий типовые события рисков данных на основе онтологии рисков данных. Содержит иерархическую классификацию событий по категориям, источникам и причинам возникновения нарушений качества данных в соответствии с признаками; описание типовых сценариев реализации; связь с затронутыми бизнес-процессами и доменами данных. Применяется при регистрации событий риска данных, проведении RCA-анализа, агрегации статистики для отчетности и заполнении карточек рисков. Обеспечивает единообразие учета и сопоставимость данных о событиях рисков данных между подразделениями и отчетными периодами

ПРИЛОЖЕНИЯ

Приложение 1

Состав и примеры факторов риска данных

Пример возможного состава факторов риска данных представлен ниже.

1. Факторы риска управления жизненным циклом данных

1.1. Недостатки процессов сбора данных:
- 1.1.1. Недостаточный контроль первичного (в том числе ручного) ввода данных
- 1.1.2. Сбои автоматизированного получения данных
- 1.1.3. Недостатки интеграции с внешними поставщиками данных

1.2. Недостатки процессов обработки и трансформации данных:
- 1.2.1. Сбои трансформации и обогащения данных
- 1.2.2. Нарушение последовательности обработки данных
- 1.2.3. Отсутствие управления изменениями в обработке данных
- 1.2.4. Недостаточное тестирование процессов обработки данных

1.3. Недостатки процессов хранения и управления данными:
- 1.3.1. Рассинхронизация хранимых/мигрируемых данных
- 1.3.2. Нарушение условий соглашений внешними провайдерами по хранению данных
- 1.3.3. Несоответствие хранилища данных бизнес-требованиям к хранению данных

1.4. Недостатки процессов распространения и предоставления данных:
- 1.4.1. Отсутствие контроля качества публикуемых данных
- 1.4.2. Недостатки управления версиями данных
- 1.4.3. Отсутствие валидации исходных данных при принятии управленческих решений

1.5. Нарушение регламентов управления данными:
- 1.5.1. Отсутствие автоматизации управления жизненным циклом данных

2. Факторы риска, связанные с организацией процессов работы с данными

2.1. Недостатки организационной модели управления данными:
- 2.1.1. Невыполнение функций Владельца данных
- 2.1.2. Неопределенность полномочий и зон ответственности по работе с данными в СУД
- 2.1.3. Отсутствие четкого разграничения зон ответственности (RACI-матрица) в процессах СУД

2.2. Неконтролируемая пользовательская обработка данных:
- 2.2.1. Использование несанкционированных ИТ-инструментов и/или алгоритмов вычислений по критичным данным
- 2.2.2. Использование несанкционированных (в том числе персональных) облачных сервисов хранения и обработки данных
- 2.2.3. Передача данных небезопасными каналами
- 2.2.4. Отсутствие инвентаризации допустимых пользовательских средств обработки критичных данных

3. Факторы риска архитектуры данных

3.1. Недостатки архитектурной модели данных:
- 3.1.1. Отсутствие описания критичных данных в корпоративной модели данных
- 3.1.2. Множественность систем – источников данных критичных данных
- 3.1.3. Технические барьеры в интеграции ИТ-систем

3.2. Недостатки управления метаданными и Data Lineage:
- 3.2.1. Неполнота/противоречивость описания терминов Бизнес-глоссария и/или Каталога данных
- 3.2.2. Отсутствие прослеживаемости происхождения данных
- 3.2.3. Отсутствие документации об алгоритмах трансформации данных

3.3. Недостатки автоматизации обработки данных:
- 3.3.1. Отсутствие необходимой автоматизации обработки потоков критичных данных
- 3.3.2. Значимый объем ручных операций в процессах обработки критичных данных
- 3.3.3. Ограниченная масштабируемость при росте объема обрабатываемых критичных данных
- 3.3.4. Отсутствие необходимой автоматизации мониторинга качества данных

4. Факторы риска, связанные с соблюдением нормативных и регуляторных требований

4.1. Несоблюдение регуляторных требований к данным:
- 4.1.1. Неспособность подтвердить работу контрольных процедур по процессам обработки данных
- 4.1.2. Нарушение установленных сроков предоставления регуляторной отчетности

4.2. Недостатки системы внутреннего контроля в части данных:
- 4.2.1. Отсутствие мониторинга изменений законодательства
- 4.2.2. Непроведение периодических самооценок риска данных
- 4.2.3. Отсутствие контроля полноты выполнения предписаний Банка России и других регуляторов по устранению замечаний по данным

Приложение 2

ПРИМЕРЫ ПО ТИПИЧНЫМ ФАКТОРАМ РИСКА ДАННЫХ *Табл. П-2-1*

Фактор риска (позиции из Приложения 1)	**Описание примера для фактора риска данных**
1.2.3. «Отсутствие управления изменениями в обработке данных»	Банк при формировании аналитической витрины для скоринговой модели использовал ETL-процесс с жестко зафиксированным перечнем продуктовых кодов (ипотека, потребительские кредиты, кредитные карты). При запуске нового продукта «Кредит под залог автомобиля» код продукта не был добавлен в справочник фильтрации ETL-процесса. В течение 2 месяцев история обслуживания около 3 500 клиентов по новому продукту не учитывалась в скоринге. Клиенты с положительной кредитной историей по автокредитам получали заниженные скоринговые баллы и относились к более консервативным сегментам. Последствия: около 12% заявок от качественных клиентов отклонены или одобрены с повышенной ставкой. Недополученный процентный доход составил приблизительно 7 млн рублей. Отток более 300 клиентов к конкурентам. Внедрение автоматической проверки полноты продуктового справочника в ETL и процедуры обязательного обновления маппинга при запуске продукта предотвратило бы потери
1.3.1. «Рассинхронизация хранимых/мигрируемых данных»	Управление риском потери данных по кредитным заявкам. Банк при внедрении CRM-системы идентифицировал риск потери данных о кредитных заявках при миграции. Вероятность была оценена как высокая (0,8) с потенциальным ущербом 50–200 млн рублей. Для митигации риска данных были внедрены: резервное копирование каждые 4 часа, параллельная работа старой и новой систем 3 месяца, автоматическая сверка данных между legacy и новой системами по контрольным суммам критичных полей. Установлен KRI – количество расхождений (целевое = 0) при ежедневной сверке. За период миграции выявлено 12 расхождений, все обнаружены в течение 4 часов и устранены без потерь. Инвестиции в проверки качества данных 4 млн руб. предотвратили потенциальные потери на 15 млн рублей
1.4.2. «Недостатки управления версиями данных»	Банк при планировании замены АБС идентифицировал риск потери контроля актуальности и качества данных, передаваемых в 17 потребляющих систем. В период миграции возникал риск рассинхронизации данных между старой и новой АБС, использования устаревших или дублированных записей. Потенциальное воздействие – принятие некорректных решений в критичных процессах (платежи, отчетность) с ущербом до 100 млн руб./день из-за использования неактуальных данных. Разработан план, предусматривал создание промежуточного слоя данных (data hub) с встроенным контролем версионности и актуальности, фиксация требований к качеству данных и временным меткам между системами, поэтапная миграция с перекрытием периодов и сверкой актуальности данных, автоматические тесты качества и консистентности для 200+ критичных потоков. Был внедрен мониторинг KRI – «Доля потоков данных с подтвержденной актуальностью и корректностью» для параллельно работающих систем. За 6 месяцев подготовки обеспечен контроль качества для 98% потоков данных, выявлено и устранено 23 критичных несоответствия в актуальности и полноте данных. При миграции все системы продолжили получать актуальные и валидированные данные, демонстрируя эффективность проактивного управления риском качества данных
1.4.3. «Отсутствие валидации исходных данных при принятии управленческих решений»	Банк при разработке стратегии регионального развития не включил в процесс оценку качества используемых данных. Риск использования некорректных данных о доходах населения не был идентифицирован, требования к качеству аналитических данных отсутствовали. Отчет для Правления готовился на основе устаревших данных Росстата без валидации и кросс-проверки с альтернативными источниками. Данные оказались формально полными, но устаревшими. Проверки качества входных данных не применялись, ответственный за верификацию не назначен. Правление одобрило программу ипотечного кредитования с целевым объемом больше 5 млрд руб., полагаясь на завышенные показатели доходов. Только через 9 месяцев при росте просрочки до 14% (вместо плановых 3%) была проведена проверка, выявившая использование устаревших данных. К этому моменту убытки составили свыше 500 млн рублей. Дальнейший анализ показал, что инвестиции в валидацию данных (около 2 млн руб.) и привлечение актуальных источников (1 млн руб.) могли предотвратить бы 95% потерь
3.2.2. «Отсутствие прослеживаемости происхождения данных»	Страховая компания при формировании управленческой отчетности для Совета директоров обнаружила расхождение показателя убыточности каско между управленческим и регуляторным отчетами на 3,7 процентного пункта. Из-за отсутствия документированного Data Lineage команда аналитиков не могла определить полный путь данных от первичных учетных систем до итоговых показателей в отчетах. Расследование причин расхождения заняло 4 недели силами рабочей группы из 6 человек: 2 аналитика, 2 дата-инженера, разработчик хранилища и бизнес-пользователь. Совокупные трудозатраты составили больше 1 000 человеко-часов, что при средней стоимости часа 1 800 руб. эквивалентно 1,8 млн рублей. Причина расхождения оказалась в различных правилах исключения регрессных выплат, применяемых на разных уровнях трансформации данных. По результатам внедрена система автоматизированного формирования Data Lineage. Определены KRI: процент отчетных показателей с задокументированным Data Lineage от источника до потребителя, со средним временем диагностики не более 16 рабочих часов

Приложение 3

СОСТАВ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ И СТАНДАРТОВ, СВЯЗАННЫХ С РИСКОМ ДАННЫХ УФР *Табл. П-3-1*

ОБЩИЕ ТРЕБОВАНИЯ
Указание Банка России от 25.12.2017 № 4662-У «О квалификационных требованиях к руководителю службы управления рисками, службы внутреннего контроля и службы внутреннего аудита кредитной организации, лицу, ответственному за организацию системы управления рисками, и контролеру негосударственного пенсионного фонда, ревизору страховой организации о порядке уведомления Банка России о назначении на должность (об освобождении от должности) указанных лиц (за исключением контролера негосударственного пенсионного фонда), специальных должностных лиц, ответственных за реализацию правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма кредитной организации, негосударственного пенсионного фонда, страховой организации, управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, микрофинансовой компании, сотрудника службы внутреннего контроля управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, а также о порядке оценки Банком России соответствия указанных лиц (за исключением контролера негосударственного пенсионного фонда) квалификационным требованиям и требованиям к деловой репутации»
КРЕДИТНЫЕ ОРГАНИЗАЦИИ
Операционная надежность: • Положение Банка России от 13.01.2025 № 850-П «Об обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» Управление операционными рисками: • Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» Для СЗКО: Положение Банка России от 02.11.2024 № 845-П «О порядке расчета величины кредитного риска банками с применением банковских методик управления кредитным риском и моделей количественной оценки кредитного риска», Приложение 2 к Положению, «Требования к качеству используемых в банковских моделях количественной оценки кредитного риска данных» – требования к составу характеристик качества данных. Указание Банка России от 03.03.2025 № 7005-У «О порядке получения банком разрешения на применение банковских методик управления кредитным риском и моделей количественной оценки кредитного риска, порядке выдачи, порядке отзыва и порядке внесения изменений в условия указанного разрешения, порядке применения банковских методик управления кредитным риском и моделей количественной оценки кредитного риска и о порядке оценки Банком России качества указанных методик и моделей»
НЕКРЕДИТНЫЕ ОРГАНИЗАЦИИ
Базовые документы: • Положение Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг) Операционная надежность: • Положение Банка России № 779-П
НЕГОСУДАРСТВЕННЫЙ ПЕНСИОННЫЙ ФОНД
Указание Банка России от 04.07.2016 № 4060-У «О требованиях к организации системы управления рисками негосударственного пенсионного фонда» – о выявлении рисков и организации процесса управления рисками, включая риски данных
ПРОФЕССИОНАЛЬНЫЕ УЧАСТНИКИ РЫНКА ЦЕННЫХ БУМАГ
Указание Банка России от 21.08.2017 № 4501-У «О требованиях к организации профессиональным участником рынка ценных бумаг системы управления рисками, связанными с осуществлением профессиональной деятельности на рынке ценных бумаг и с осуществлением операций с собственным имуществом, в зависимости от вида деятельности и характера совершаемых операций» – определение рисков профессионального участника и требования к регламенту управления рисками. Методические рекомендации Банка России от 29.11.2024 № 20-МР, «Методические рекомендации Банка России об организации профессиональными участниками рынка ценных бумаг системы управления операционным риском» – отражение рисков, ведение базы событий, ведение реестра операционных рисков и рекомендации по самооценке
КЛИРИНГОВЫЕ ОРГАНИЗАЦИИ, ЦЕНТРАЛЬНЫЕ КОНТРАГЕНТЫ, ЦЕНТРАЛЬНЫЙ ДЕПОЗИТАРИЙ И РЕПОЗИТАРИИ
Положение Банка России от 02.10.2023 № 827-П «О требованиях к управлению рисками клиринговых организаций, центральных контрагентов, центрального депозитария и репозитариев в части управления операционным риском» – состав действий по управлению операционным риском и состав сведений о событиях операционного риска

Приложение 4

Пример описания потоков данных в рамках применения ПВР

В рамках исполнения требований абзаца восьмого[1] пункта 2.3 Положения Банка России № 845-П[2] и Приложения 2 к указанному Положению, банк, применяющий подход на основе внутренних рейтингов (далее – ПВР), во внутренних методиках, регламентирующих процессы управления данными и обеспечения их качества в рамках применения ПВР, в том числе приводит **описание потоков данных,** используемых в расчете величины кредитного риска с применением ПВР.

Элементами описания потоков данных являются технологическая схема организации (карта) потоков данных, а также таблица с описанием потоков данных.

Иллюстративные примеры таблицы и схемы (карты) приведены далее.

ПРИМЕР ТАБЛИЦЫ ОПИСАНИЯ ПОТОКОВ ДАННЫХ *Табл. П-4-1*

№	Данные	Система-источник	Витрина-источник*	Система-потребитель	Витрина – выходной объект данных**
1	Сделки типа X	ИТ-система 1	deals_repo	ИТ-система 2	deals
2	Остаток кредитного лимита	ИТ-система 2	limits_ucl	ИТ-система 1	limits
…					
18	Данные о дефолтах корпоративных заемщиков	ИТ-система 7	default_base_corp	ИТ-система 9	defaults
…					
23	Результаты расчета RWA	Калькулятор расчета RWA	rwa_calc	Хранилище данных	rwa
…					

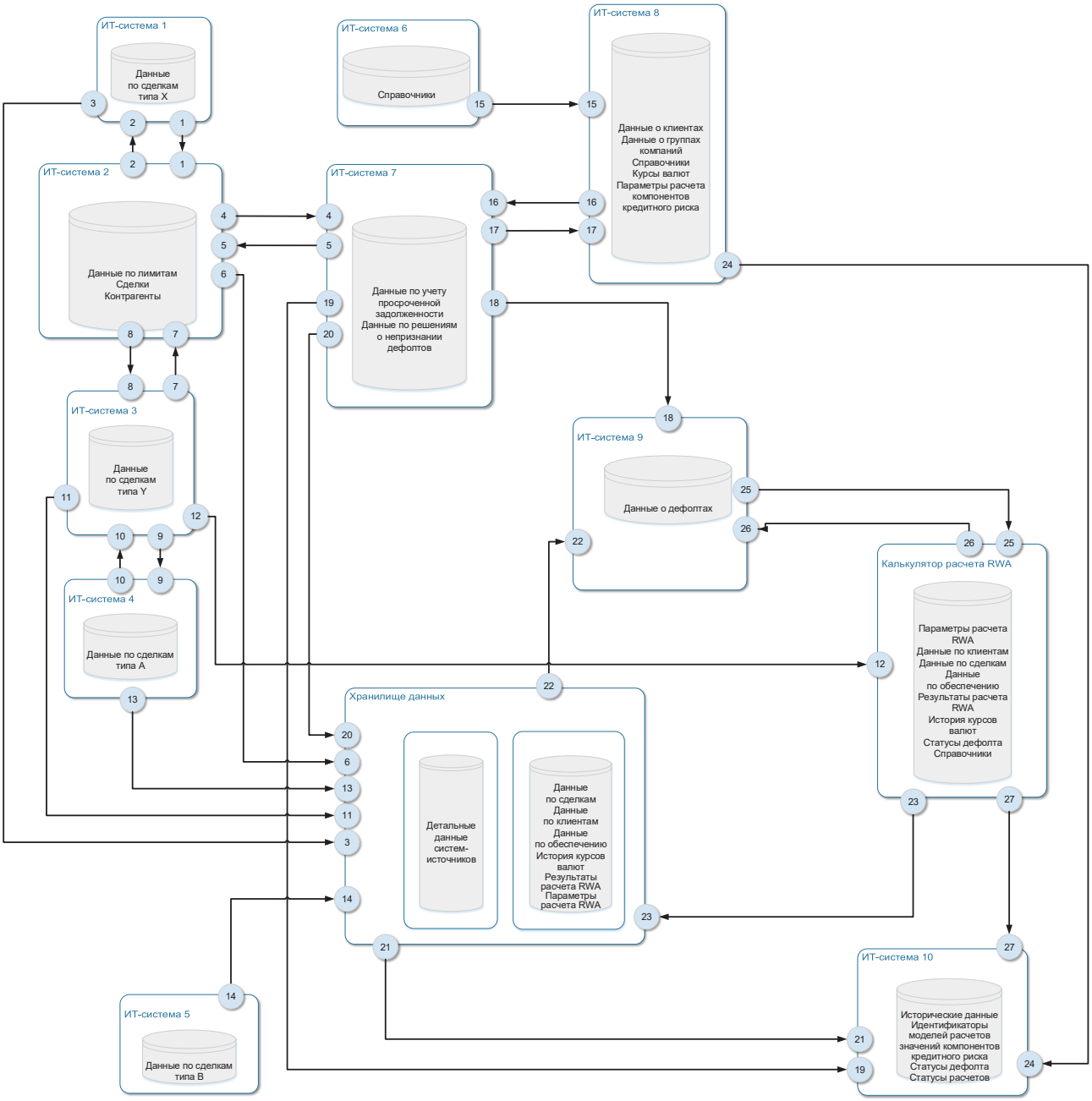
** В отдельной таблице приводится атрибутивный состав витрины-источника данных.*
*** В отдельной таблице приводится атрибутивный состав витрины.*

[1] «Банк в соответствии с требованиями к качеству данных, установленных приложением 2 к настоящему Положению, разрабатывает процедуры и методики оценки, контроля и повышения качества данных, используемых для построения и применения рейтинговых систем (в том числе для применения во внутренних процессах принятия решений и управления кредитным риском <…>) и для оценки активов и расчета нормативов достаточности капитала».

[2] Положение Банка России от 02.11.2024 № 845-П «О порядке расчета величины кредитного риска банками с применением банковских методик управления кредитным риском и моделей количественной оценки кредитного риска».

ПРИМЕР ТЕХНОЛОГИЧЕСКОЙ СХЕМЫ ОРГАНИЗАЦИИ (КАРТА) ПОТОКОВ ДАННЫХ

Табл. П-4-2



Приложение 5

Описание ролей, вовлеченных в процесс «Управление рисками данных»

Данный перечень не является исчерпывающим. Каждая организация в силу специфики деятельности может иметь свой собственный набор ролей (включая объединение нижеуказанных ролей).

Табл. П-5-1

Роль участника СУД	Описание роли
Архитектор данных	Основными задачами Архитектора данных являются: • обеспечение комплексного подхода к моделированию архитектуры данных для оптимизации процессов работы с данными; • обеспечение координации вопросов, связанных с актуализацией определений данных и их моделей; • разработка стандартов моделирования и построения Архитектуры данных организации; • определение требований к организации слоев сбора, хранения, обработки, слоев предоставления и интеграции данных; • разработка схемы потоков данных в организации; • проектирование целевой Архитектуры данных в соответствии со стратегией организации
Владелец данных	Ответственное подразделение и (или) назначенный руководитель/сотрудник организации, осуществляющий управление закрепленными за ним объектами данных и ответственный за качество этих данных. Владелец данных назначается решением уполномоченного Коллегиального органа по управлению данными организации. Основными задачами Владельца данных являются: • обеспечение консолидации потребностей пользователей в данных, определение приоритетов их удовлетворения, формирование планов развития данных; • определение правил и методологий формирования данных, а также способа появления данных (вручную, автоматически, через интеграцию); • согласование изменений в структуре и составе данных; • управление требованиями к доступности данных, эффективностью процесса производства и переиспользования данных; • формирование и практическая реализация методологии управления качеством данных в организации, определение критериев качества данных; • приведение качества данных к соответствующим требованиям и осуществление контроля их исполнения; • определение, валидация проверок качества данных и их алгоритмов; • определение критичности данных; • координирование методологической поддержки пользователей данных; • проведение оценки рисков и влияния на бизнес при изменении данных; • модерирование разрешения разногласий, инцидентов и проблем с объектами данных, находящимися в зоне ответственности Владельца данных; • назначение на роли Эксперта по качеству данных и Офицера данных; • выполнение работ по накоплению и актуализации знаний о данных (в Бизнес-глоссарии данных, Каталоге данных и так далее); • контроль прохождения обучения по управлению данными сотрудников, вовлеченных в управление качеством данных и использование данных
Директор по управлению данными / Директор по данным	Обеспечивает функционирование деятельности по управлению данными в организации. Основными задачами Директора по управлению данными являются: • представление на согласование/утверждение уполномоченному Коллегиальному органу основных направлений развития системы управления данными в организации; • разработка и внедрение стратегии, политики и стандартов управления данными; • формирование целей и управление ожиданиями от функции управления данными у пользователей данных; • информирование заинтересованных сторон о состоянии качества данных, системы управления данными и эффективности процессов управления данными; • обеспечение соответствия управления данными требованиям регуляторов и бизнеса; • развитие культуры управления данными в организации; • участие в организации обучения сотрудников организации по вопросам, связанным с процессами управления данными

Роль участника СУД	Описание роли
Коллегиальный орган по управлению данными	Уполномоченный Коллегиальный орган по управлению данными. Полномочия Коллегиального органа должны устанавливаться соответствующим приказом по организации. Основными задачами Коллегиального органа по управлению данными являются: • рассмотрение и утверждение ключевых решений по управлению данными; • обеспечение координации и взаимодействия подразделений по вопросам управления данными; • утверждение стратегических целей в области данных; • утверждение политики управления данными; • утверждение показателей эффективности; • утверждение критериев назначения на роль Владельца данных; • медиация и арбитраж спорных вопросов и ситуаций в процессах управления данными
Офис Директора по управлению данными / Директора по данным	Основными задачами Офиса Директора по управлению данными являются: • разработка (развитие) ролевой/функциональной/организационной моделей управления данными, разработка и внедрение политики, процессов, методологии и методик управления данными в организации, соглашений/регламентов работы с данными в организации; • осуществление мониторинга выполнения функций управления данными и использования данных в организации; • информирование пользователей о состоянии качества данных в организации; • определение КПЭ по управлению качеством данных, подходов к методике расчета и установлению целевых значений; • организация и проведение оценки зрелости управления данными; • организация и обеспечение эффективности проверок качества данных; • организация процессов обучения сотрудников организации по тематике управления данными, разработка метрик и отчетов об эффективности управления данными
Офицер данных (дата-стюард)	Основными задачами Офицера данных являются: • исполнение задач Владельца данных на операционном уровне в своей зоне ответственности; • ведение и обеспечение качества справочных и/или основных данных; • формирование требований к качеству данных, согласование с заинтересованными сторонами; • подготовка предложений к требованиям по методологии управления качеством данных по направлению своей зоны ответственности; • валидация результатов проверок качества данных по объектам данных и оценка эффективности проверок качества данных; • приоритизация инцидентов качества данных, разработка и реализация планов по их устранению
Пользователь данных	Основными задачами Пользователя данных являются: • использование доступных данных для выполнения должностных обязанностей; • формирование требований к составу и качеству данных; • предложение Владельцу данных дополнительных требований к составу и качеству данных; • инициация инцидентов в случае нарушения показателей качества данных и нарушения метрик соглашений по обмену данными, предоставления сведений для инцидентов по данным; • участие в оценке операционного риска некачественных данных и влияния на бизнес-процесс, в котором он использует данные, а также в тестировании данных и валидации изменений; • предоставление обратной связи по удобству и эффективности использования данных
Эксперт по качеству данных	Эксперт по качеству данных играет ключевую роль в обеспечении целостности, точности и полноты данных. Основными задачами Эксперта по качеству данных являются: • разработка предложений по проверкам качества данных, алгоритмам и сценариям устранения нарушений; • мониторинг качества данных и идентификация инцидентов по качеству данных; • координация и участие в процессе решения инцидентов на уровне ИТ-системы, включая анализ первопричин и разработку превентивных мер; • анализ и маршрутизация инцидентов качества данных; • предоставление отчетов по решению инцидентов качества данных; • координация решений инцидентов на уровне Офицера данных и Владельца данных; • разработка сценариев устранения нарушений в данных; • управление инцидентами: анализ причин, информирование заинтересованных сторон об инцидентах и их причинах согласно установленному процессу; • контроль устранения критичных инцидентов качества данных и своевременное информирование о критичных инцидентах Владельцев данных и других заинтересованных сторон

Приложение 6

Рекомендации по содержанию карточки события риска данных

КАРТОЧКА РИСКА ДАННЫХ *Табл. П-6-1*

КЛАССИФИКАЦИЯ СОБЫТИЯ РИСКА ДАННЫХ	
Регистрационные данные	
• ID события риска данных	[Автогенерация ID]
• Инцидент качества данных	[Множественный выбор из списка инцидентов]
• ID риска	[Ссылка на карточку риска]
• Дата и время регистрации события	[Дата/время]
• Дата и время реализации события	[Дата/время]
• Дата и время выявления события	[Дата/время]
• Дата и время окончания события	[Дата/время]
• Подразделение источник о события	[Код / Название подразделения]
• Подразделение, выявившее событие	[Код / Название подразделения]
• Статус события	[Анализ/Оценка/Устранение/Закрыто]
Классификация и группировка событий	
• Категория источника	[Человеческий фактор / Процесс / Система / Внешние]
• Подкатегория	[Зависимый список подкатегорий]
• Тип события	[Из Классификатора типовых событий рисков данных]
Затронутые объекты	
• Затронутые ИТ-системы	[Множественный выбор из списка ИТ-систем]
• Затронутые данные	[Из Каталога данных]
• Направление деятельности	[Из реестра направлений деятельности]
• Затронутые процессы	[Бизнес-процессы]
• Нарушенные характеристики качества данных	[Множественный выбор характеристик качества данных]
АНАЛИЗ ВОЗДЕЙСТВИЯ	
Оценка воздействия	
• Косвенные потери	[Сумма] (для распределения)
• Потенциальные потери	[Оценка суммы]
• Общий ущерб	[Авторасчет]
• Остаточный риск**	[Сумма]
• Регуляторное воздействие	[Да/Нет], [Описание]
Нефинансовое воздействие	
• Репутационное воздействие	[Низкое/Среднее/Высокое/Критическое]
• Регуляторное [Да/Нет + описание]	[Да/Нет], [Описание]
• Операционное воздействие	[Время простоя / объем затронутых операций]
• Влияние на клиентов	[Количество затронутых клиентов]

РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

РОЛЬ	СИСТЕМА/ПРОЦЕСС	ФИО	% ОТВЕТСТВЕННОСТИ	СУММА РИСКА
Владелец данных	[автозаполнение по домену]	[автозаполнение]	[%]	[авторасчет]
Владелец ИТ-системы	[по системе-источнику]	[автозаполнение]	[%]	[авторасчет]
Владелец процесса	[по бизнес-процессу]	[автозаполнение]	[%]	[авторасчет]

• Обоснование распределения: [текстовое поле]

УЧЕТ ПОТЕРЬ	
• Вид потери	[согласно по п. 3.11]
• Дата учета потери	[Дата]
• Бухгалтерская запись	[ID записи, счет, сумма, валюта]
• Сумма валовых прямых потерь (накопительно)	[Сумма, валюта]
• Сумма чистых потерь	[Сумма, валюта]
РЕАГИРОВАНИЕ И УСТРАНЕНИЕ	
Обнаружение и информирование заинтересованных сторон	
• Участники реагирования	[Список вовлеченных]
• Хронология действий	[Хронология событий]
Анализ корневых причин (RCA)	
• Непосредственная причина	[Что произошло]
• Корневая причина	[Выбор из типового каталога причин КД]
• Способствующие факторы	[Описание того, что усугубило]
• Цепочка событий	[Последовательность событий во времени]

ПЛАН КОРРЕКТИРУЮЩИХ ДЕЙСТВИЙ

МЕРОПРИЯТИЕ	УСТРАНЯЕМАЯ ПРИЧИНА	ОТВЕТСТВЕННЫЙ	СРОК	СНИЖЕНИЕ РИСКА
[описание]	[ссылка на анализ причин RSA]	[из матрицы ответственности]	[дата]	[% снижения]

КОММУНИКАЦИИ И УВЕДОМЛЕНИЯ	
• Внутренние уведомления	[Руководство / Участники коллегиальных органов / Подразделения]
• Внешние уведомления	[Регулятор/Клиенты/Партнеры]
• Сроки уведомлений	[Список фактов уведомлений]
КОНТРОЛЬ УСТРАНЕНИЯ	
Верификация	
• Дата фактического устранения	[Дата]
• Подтверждение устранения	[Тестирование/верификация]
• Остаточный риск	[Оценка после устранения]
Извлеченные уроки	
• Рекомендации	[Предложения по улучшению]
• Обновление контролей	[Новые/измененные контроли]
• Изменение процессов	[Корректировка процедур]
ССЫЛКИ	
• Связанные риски	[Другие затронутые риски]
• Связанные события	[Предыдущие похожие события]
• Инциденты ИТ	[ID из Service Desk]
• Документация	[Приложенные файлы/отчеты]
ИСТОРИЯ ИЗМЕНЕНИЙ	
• Изменение в карточке события	[Дата, время, ФИО, Описание действия]

** Для кредитных организаций классификация по источникам операционного риска производится в соответствии пунктом 3.3 главы 3 Положения Банка России № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».*

*** Остаточный риск – это риск, с которым организация продолжает деятельность после внедрения/функционирования контролей и мероприятий по снижению риска. Сумма фактического убытка используется для учета и анализа произошедших событий, а оценка остаточного риска используется для управленческих решений: нужны ли дополнительные меры или целесообразно изменение профиля деятельности.*

Приложение 7

Рекомендации по содержанию карточки риска данных

КАРТОЧКА РИСКА ДАННЫХ *Табл. П-7-1*

ИДЕНТИФИКАЦИЯ И РЕГИСТРАЦИЯ	
• ID риска данных	[Автогенерация ID]
• Наименование риска	[Текст до 100 символов]
• Описание риска	[Развернутое описание]
• Статус риска	[Идентифицирован / В оценке / Принят / В обработке / Закрыт]
• Дата и время регистрации	[Дата и время]
• Дата обновления	[Автообновление]
• Источник идентификации	[Проект/Аудит/Инцидент/Регулятор/Подразделение]
КЛАССИФИКАЦИЯ	
Таксономия риска	
• Критичный элемент данных (CDE)	[Справочник CDE]
• Категория OP	[Классификатор операционных рисков]
• Тип риска данных	[Качество / Утрата / Несанкционированный доступ/...]
• Бизнес-процесс	[Справочник процессов]
• Операция/шаг процесса	[Детализация процесса]
Объекты воздействия	
• Категории данных	[ПДн / Финансовая отчетность / Коммерческая тайна/...]
• Уровень конфиденциальности	[Общедоступные/Служебные/Конфиденциальные/Секретные]
• ИТ-системы	[Справочник систем]
• Нарушаемые характеристики ка-чества данных	[Полнота/Точность/Актуальность/...]
ВЛАДЕНИЕ И ОТВЕТСТВЕННОСТЬ	
• Владелец риска	[Должность/подразделение]
• Владелец данных	[Руководитель домена данных]
• Владелец ИТ-системы	[Ответственный за систему]
• Матрица RACI	[Таблица распределения ролей]
ОЦЕНКА РИСКА	
Исходный риск (Inherent)	
• Вероятность (I)	[1–5 шкала]
• Воздействие (I)	[1–5 шкала]
• Уровень (I)	[Авторасчет по матрице]
Остаточный риск (Residual)	
• Методика оценки	[Описание подхода]
• Эффективность контролей	[% снижения]
• Вероятность (R)	[1–5 шкала]

• Воздействие (R)	[1–5 шкала]
• Уровень (R)	[Авторасчет по матрице]
Допустимость	
• Целевой уровень	[Порог аппетита к риску]
• Соответствие аппетиту	[В пределах / Превышен]
КОНТРОЛИ И МОНИТОРИНГ	
• КИРД	[Список показателей]
• Пороговые значения	[Триггеры для информирования заинтересованных сторон: КИРД – Уровень]
• Тип контролей	[Превентивный/Детективный/Корректирующий]
• Частота контроля	[Периодичность]
СТРАТЕГИЯ ПО РИСКУ	
• Стратегия	[Снижение/Принятие/Избежание/Передача]
• План мероприятий	[Список действий]
• Ответственные	[По каждому мероприятию]
• Сроки	[Плановые даты]
• Статус выполнения	[Не начато / В работе / Завершено]
СВЯЗИ	
• События риска	[Ссылки на ID событий]
• Статистика событий	[Частота/ущерб/тренды]
• Регуляторные требования	[845-П/850-П/716-П/...]
• Периодичность пересмотра	[Квартал/год]
• Дата последнего пересмотра	[Дата пересмотра]
• Дата пересмотра	[Плановая дата]

Приложение 8

Описание процесса «Управление рисками данных»

Табл. П-8-1

Процесс/подпроцесс	Описание процесса/подпроцесса
1. РАЗРАБОТКА МЕТОДОЛОГИИ УПРАВЛЕНИЯ РИСКАМИ ДАННЫХ	
1.1. Разработка/ совершенствование методологии соотнесения рисков данных с СУР организации	Включает соотнесение рисков данных с классификаторами СУР, производится единообразное описание проблем качества данных в контексте классификатора событий операционного риска. Производится разработка правил описания и классификации типовых событий рисков данных, формализация критериев существенности для признания инцидента качества данных событием риска данных и закрепление ответственности владельцев данных за идентификацию и информация о наступлении событий при наличии утвержденного классификатора СУР и определенных границ периметра рисков. Результат: D064 Регламент процесса управления рисками в области данных, D166 Реестр ответственных за риски данных, D174 Классификатор типовых событий рисков данных
1.2. Описание/актуализация процесса управления рисками данных	Описание и актуализация процесса управления рисками данных обеспечивает поддержание методологии в актуальном состоянии и ее соответствие регуляторным требованиям на основе мониторинга изменений требований Банка России, ИТ-ландшафта и бизнес-процессов организации. Включает анализ и оценку влияния изменений на риски данных, инициацию корректировок методологии, описания процессов, проведение оценки риска изменений с учетом особенностей объектов данных и синхронизации с требованиями СУР. Результат: D064 Регламент процесса управления рисками в области данных, D170 Запросы на изменения КИРД по рискам данных
1.3. Определение и настройка КИРД, установка пороговых значений и правил информирования	Определение и настройка КИРД обеспечивает предупреждение о потенциальных событиях риска данных, интегрированных в систему ключевых индикаторов риска СУР. Включает формирование реестра индикаторов, установление сигнальных и контрольных пороговых значений и определение порядка коммуникаций (оповещения) при нарушении порогов и при наличии технической возможности мониторинга. Результат: D160 Реестр ключевых индикаторов риска данных, D170 Запросы на изменения КИРД по рискам данных
1.4. Идентификация и регистрация рисков данных в СУР	Идентификация и регистрация рисков данных в СУР обеспечивает систематическое выявление и формализованное описание потенциальных рисков в области данных на основе анализа бизнес-процессов, информационных систем, потоков данных, результатов самооценки и аудиторских проверок. Включает проведение первичной идентификацию рисков данных, их соответствующей классификации и оформление карточек риска данных. Результат: D173 Карточка риска данных, D174 Классификатор типовых событий рисков данных
2. ВЫЯВЛЕНИЕ И РЕГИСТРАЦИЯ СОБЫТИЙ РИСКА ДАННЫХ	
2.1. Выявление среди инцидентов качества данных потенциальных событий риска данных (из ИТ-систем или других источников)	Выявление среди инцидентов качества данных потенциальных событий риска данных обеспечивает формирование первичного пула событий-кандидатов для квалификации на основе уведомлений систем мониторинга, сведений о сбоях ETL-процессов, ошибках ручного ввода и нарушениях условий соглашений по обмену данными. Это касается данных и сведений, поступающих из ИТ-систем организации, а также из иных источников. Включает автоматизированный сбор информации и сбор информации от экспертов об инцидентах качества данных, обобщение уведомлений о превышении пороговых значений КИРД. Результат: D168 Отчет о срабатывании проверок качества данных, D074 Реестр проблем, D173 Карточка риска данных
2.2. Анализ инцидентов качества данных и их типизация по степени влияния на бизнес-процессы	Квалификацию событий-кандидатов (инцидентов качества данных) для регистрации в базе операционных рисков и их типизацию для последующей регистрации события риска и риска данных организации, если необходимо. Включает проверку порога существенности потерь, классификацию по онтологии риска данных с определением вида и источника, документированное отсеивание несущественных инцидентов качества данных. Результат: D158 Карточка события риска данных
2.3. Предварительная оценка последствий события риска данных	Предварительная оценка последствий события обеспечивает определение приоритета и очередности исследования в рамках СУР на основе сведений о событии риска данных и информации о затронутых бизнес-процессах. Может включать определение типа и предварительной величины потерь, оценку влияния на непрерывность критичных процессов, регуляторную отчетность и клиентский сервис, присвоение приоритета события при наличии методологии оценки потерь и карты критичных бизнес-процессов организации. Результат: D158 Карточка события риска данных
2.4. Фиксация событий риска данных	Включает создание карточки события риска данных, и, как следствие, если необходимо, может создаваться описание нового риска данных посредством карточки риска данных. Производится заполнение обязательных атрибутов карточек и обеспечение прослеживаемости от момента выявления до завершения исследования по событию риска. Результат: D158 Карточка события риска данных, D173 Карточка риска данных
3. ОБСЛЕДОВАНИЕ СОБЫТИЙ РИСКА ДАННЫХ И ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ РИСКА	
3.1. Анализ корневых причин (RCA) событий риска данных	Анализ корневых причин событий риска данных обеспечивает идентификацию первопричин инцидентов качества данных для формирования корректирующих мероприятий на основе карточки события риска данных. Включает проведение исследования с применением методологии RCA, категоризацию причин по типам (дефекты метаданных, ошибки интеграции, человеческий фактор, внешние факторы), документирование причинно-следственных связей при наличии доступа к логам систем и метаданным затронутых объектов. Результат: D159 Отчеты RCA по событиям риска данных, D173 Карточка риска данных

Процесс/подпроцесс	Описание процесса/подпроцесса
3.2. Оценка влияния и приоритизация инцидентов качества данных на смежные процессы и ИТ-системы	Производится оценка влияния и приоритизация инцидентов качества данных на смежные процессы и ИТ-системы обеспечивает полноту определения периметра влияния события риска на процессы организации. Результаты оценки и приоритизации используются для расчета совокупных потерь на основе карт Data Lineage и результатов RCA-анализа. Может включать анализ распространения некорректных данных по информационным системам, оценку вторичных рисков при наличии актуальных карт происхождения данных и реестра критичных бизнес-процессов. Результат: D159 Отчеты RCA по событиям риска данных, D044 Отчет о рисках, связанных с низким качеством данных, D173 Карточка риска данных
3.3. Самооценка рисков данных	Самооценка рисков данных и качества работы контрольных процедур данных обеспечивает формирование профиля рисков данных организации на основе результатов процедуры самооценки операционного риска, реестра критичных информационных активов и бизнес-процессов. Включает идентификацию присущего риска данных, оценку дизайна и операционной эффективности контрольных процедур по объектам данных, расчет остаточного уровня риска при наличии утвержденной методологии, актуального каталога данных и матрицы проверок качества данных. Результат: D044 Отчет о рисках, связанных с низким качеством данных, D173 Карточка риска данных
3.4. Документирование результатов исследований и регистрация выявленных рисков данных	Формирование заключения по результатам исследования позволяет определить недостатки контрольной среды и создать рекомендации по предотвращению повторных инцидентов качества данных на основе результатов RCA-анализа, оценки влияния и подтвержденных потерь. Включает подготовку структурированного отчета, формулирование рекомендаций по устранению коренных причин, согласование с владельцем данных и риск-менеджментом при наличии завершенного исследования и верифицированных данных о потерях. Результат: D159 Отчеты RCA по событиям риска данных, D173 Карточка риска данных
4. РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПЛАНОВ МЕРОПРИЯТИЙ ПО СНИЖЕНИЮ РИСКА ДАННЫХ	
4.1. Координация исправления данных и причин инцидентов качества данных	Координация исправления данных и причин инцидентов качества данных обеспечивает восстановление качества пострадавших данных. Включает организацию оперативных мер по устранению непосредственных причин, регистрацию связанных инцидентов качества данных (если необходимо). Результат: D074 Реестр проблем, D167 Отчет о статусе планов устранения проблем качества данных, D173 Карточка риска данных
4.2. Формирование проектов/инициатив по совершенствованию процессов обработки данных и повышению качества данных	Формирование проектов/инициатив по совершенствованию процессов обработки данных обеспечивает устранение причин инцидентов качества данных и развитие контрольной среды на основе результатов RCA-анализа и выявленных недостатков. Включает разработку корректирующих мероприятий, проектирование новых правил валидации, доработку контрольных процедур, ETL-процессов. На данном этапе может происходить объединение сформированных проектов/инициатив в стратегию развития СУД в соответствии с установленными приоритетами. Результат: D101 Стратегия и план развития СУД в части минимизации рисков данных, D074 Реестр проблем
4.3. Координация выполнения проектов/инициатив с владельцами данных и процессов	Координация проектов/инициатив по улучшению процессов обработки данных обеспечивает взаимодействие между проектами/инициативами для достижения системного результата. Включает мониторинг статуса выполнения, контроль соблюдения сроков ответственными исполнителями, формирование периодической отчетности, уведомление о несоответствиях или критических событиях в процессе выполнения. Результат: D167 Отчет о статусе планов устранения проблем качества данных, D173 Карточка риска данных
4.4. Анализ и оценка эффективности КИРД и мероприятий по рискам данных	Анализ и оценка эффективности мониторинга КИРД и реализации мероприятий по рискам данных обеспечивает подтверждение достижения целевого уровня остаточного риска на основе данных мониторинга КИРД и результатов внедренных контрольных процедур. Включает контроль выполнения планов реализации, повторную оценку, анализ динамики срабатывания индикаторов риска после реализации улучшений, инициирование дополнительных мер при недостаточной результативности. Результат: D047 Отчет по эффективности мер повышения качества данных, D161 Отчет об эффективности КИРД, D173 Карточка риска данных
5. МОНИТОРИНГ РИСК-ОТЧЕТНОСТИ И ИНФОРМИРОВАНИЕ	
5.1. Подготовка сведений для включения в отчетность по СУР	Подготовка сведений для включения сведений по рискам данных в сводную отчетность по рискам обеспечивает формирование полной информации о рисках данных. Включает агрегацию статистики событий риска данных, в соответствие с D174 Классификатор типовых событий рисков данных, формирование рейтингов уязвимости процессов, возможность подготовки выборки событий для обязательной отчетности Банку России при наличии накопленных данных за отчетный период. Результат: D165 Отчетность и Dashboard по рискам данных, D043 Отчет о проблемах качества данных, D173 Карточка риска данных
5.2. Информирование коллегиальных органов управления и заинтересованных сторон о рисках данных	Информирование коллегиальных органов управления о рисках данных обеспечивает осведомленность высшего руководства о состоянии профиля рисков и эффективности системы управления данными на основе агрегированной аналитической отчетности. Включает подготовку отчетов для коллегиальных управляющих органов организации, выделение критических событий, существенных исключений и негативных трендов индикаторов при наличии сформированной отчетности за период и актуальных данных мониторинга. Результат: D165 Отчетность и информационных панелей по рискам данных, D043 Отчет о проблемах качества данных
5.3. Пополнение базы знаний по событиям риска данных	Пополнение базы знаний и сценариев стресс-тестирования обеспечивает развитие корпоративной базы знаний и совершенствование моделей оценки риска данных на основе накопленной статистики событий и результатов RCA-расследований. Может включать систематизацию опыта управления инцидентами качества данных, обновление библиотеки типовых угроз и сценариев, актуализацию классификации типовых событий риска данных, формирование исторических рядов потерь для калибровки моделей стресс-тестирования при наличии завершенных расследований и верифицированных данных. Результат: D169 База знаний по управлению рисками данных, D174 Классификатор типовых событий рисков данных

Приложение 9

Типовые проблемы и подходы к их решению

Табл. П-9-1

Название и описание типовой проблемы	Подходы к решению
Разрозненность оценки рисков данных и операционных рисков приводит к недооценке критических нарушений в качестве данных и финансовым потерям Описание: риск-менеджеры оценивают операционные риски без учета зависимости от риска данных. Отсутствует общая методология оценки, что приводит к пропуску критических рисков и неэффективному распределению ресурсов на уменьшение влияние события риска	**Подход 1. «Интегрированная карта рисков с зависимостями от рисков данных».** Руководитель одного из подразделений инициировал создание единой таксономии, где риски данных стали подкатегорией операционных рисков с четкими связями. Директор по данным со своим Офисом установил соответствие между критичными активами по бизнес-процессам и рисками данных через специализированную кросс-таблицу. Теперь, например, при оценке риска сбоя платежной системы есть возможность оперативно учитывать зависимость от справочника банков-корреспондентов и риск его неактуальности. Владельцы данных участвуют в ежемесячных сессиях Комитета по рискам, представляя оценку критичности своих доменов. По результатам оценки полученного эффекта от нового подхода Комитет по рискам утвердил требование включать раздел «Риски данных» во все оценки рисков. В результате такого подхода в течение 9 месяцев произошло снижение операционных потерь на 25% за счет превентивных мер по обеспечению качества данных
Отсутствие прозрачного механизма определения критичности инцидентов качества данных. Описание: оценка критичности инцидента качества данных может занимать занимает от 3 часов до 4 рабочих дней. За это время некорректные данные распространяются по десяткам систем. Отсутствие механизм быстрой оценки критичности, что приводит к неверной приоритизации и росту ущерба	**Подход 1. «Единый процесс первичной оценки для инцидентов качества данных».** В страховой компании столкнулись с ситуацией, когда инциденты качества данных с расчетом страховых премий оценивались 4 дня, хотя критичность этого процесса и соответствующий SLA были заранее определены, за это время ошибочные данные попали в несколько ключевых систем получателей данных и исправление этой ситуации оказалось довольно трудоемким и чувствительным для бизнес-процессов страховой компании. Директор по рискам совместно с Директором по управлению данными разработали интегрированный процесс экспресс-оценки на основе матрицы классификации критичности инцидентов качества данных. Была создана дежурная группа, в которой работают риск-менеджер и Эксперт по качеству данных. При поступлении инцидента качества данных дежурная группа обязана в пределах 60 минут подтвердить или скорректировать уже установленную критичность и приоритет на основе заранее согласованного SLA, а не проводить первичную оценку с нуля. Оценка производится по перечню: операционное влияние (количество затронутых процессов), влияние на данные (объем и критичность), причина появления инцидента качества данных. Владельцы данных при участии Директора по управлению данными заранее классифицировали все критические процессы и источники данных по шкале влияния на операционные процессы и SLA-требованиям. Так, например, справочник тарифов получил максимальную оценку 10 баллов из 10, так как влияет на выставление счетов, отчетность и клиентский опыт – и для него установлен SLA золотого часа: первая реакция – не позднее 60 минут с момента обнаружения. Офис Директора по данным разработал дерево решений, где каждая комбинация «тип инцидента + критичность данных» имеет предустановленный приоритет и действия, соответствующие SLA, а не требует принятия решений на лету. Так было внедрено правило золотого часа, в течение которого дежурная группа должна подтвердить/применить заранее заданный приоритет и запустить изоляцию проблемных данных. К этой идее присоединился Руководитель службы внутреннего контроля и добавил этап проверки регуляторных рисков по персональным данным и ПОД/ФТ – в рамках уже утвержденной матрицы критичности и SLA. В результате организационного развития среднее время подтверждения приоритета и запуска реагирования сократилось до 50 минут, число критических инцидентов качества данных с каскадным эффектом – на 68%, оценка экономии от предотвращенного ущерба составила около 140 млн руб. за первый год

ГЛОССАРИЙ

Термин	Определение
Анализ происхождения данных (Data Lineage)	Возможность по диаграмме потоков данных отследить происхождение и преобразования определенных элементов данных на пути от системы-источника к системе-потребителю
Аналитика самообслуживания (Self service analytics)	Форма бизнес-аналитики, где бизнес-пользователи могут самостоятельно выполнять запросы к нужным данным и генерировать обобщающие отчеты
Аналитические данные	Данные, полученные и обработанные из основных, транзакционных и справочных данных с использованием специальных методов и инструментов и использующиеся для принятия решений в организации
Аналитический слой данных (Analytics Data Layer)	Слой архитектуры данных, обеспечивающий трансформацию, агрегацию и обогащение подготовленных данных для создания витрин, показателей и аналитических моделей, функционирует совместно с семантическим слоем, используя его бизнес-определения
Архитектура и моделирование данных (Data Architecture, Data Modeling)	Архитектура данных определяет концептуальные решения по управлению данными в соответствии со стратегией организации и устанавливает соответствующие стратегические требования к данным и проектным решениям в области данных. Включает корпоративную модель данных и архитектуру потоков данных. Корпоративная модель данных включает модели данных организации, выполненные на концептуальном, логическом и физическом уровнях абстракции. Управление архитектурой данных отражает информационные потребности критически важных бизнес-процессов в виде метаданных, которые необходимы для управления данными. Моделирование данных – процесс выявления, анализа, представления и распространения требований к данным в форме модели данных (описания структуры и содержания данных)
Безопасность данных (Data Security)	Набор процессов и технологий, направленных на защиту данных от несанкционированного доступа, изменения, раскрытия или уничтожения на протяжении всего жизненного цикла данных. Обеспечивает конфиденциальность, целостность и доступность, шифрование данных, соответствие нормативным требованиям и лучшим практикам по защите информации, планирование, разработку и осуществление политики и процедур для аутентификации, авторизации и доступа пользователей, управление инцидентами безопасности данных и аудит информационных ресурсов организации
Бизнес-аналитика (Business intelligence (BI)	Деятельность бизнес-пользователя по анализу данных и формированию предложений для бизнеса, которую облегчают различные аналитические инструменты и приложения, а также хранилище и витрины данных
Бизнес-глоссарий данных	Иерархический словарь бизнес-терминов данных, в котором структурированно хранится информация об атрибутах данных, требованиях к ним, к проверкам их качества, фиксируется назначение ответственного за данные
Внешние данные	Данные из внешних относительно организации источников, получаемые (закупаемые) у внешних контрагентов для использования в организации
Внутренние данные	Данные, формируемые в системах организации на основе внешних данных или создаваемые в процессе выполнения функций организации
Диаграмма потоков данных (Data Flow Diagram (DFD)	Графическое представление потоков данных и преобразования данных, применяемые по мере перемещения данных от входа в информационную систему к ее выходу. Ключевые элементы диаграммы: • процессы, работы или функции, выполняемые в отношении данных; • места хранения данных; • внешние сущности – объекты вне информационной системы, являющиеся ее источниками или приемниками данных; • потоки данных – движение данных между процессами, местами хранения и внешними сущностями
Доступ к данным	Возможность пользователей получать необходимые данные с учетом их роли, полномочий и потребностей. Процесс предоставления доступа должен быть безопасным, управляемым и соответствовать политике конфиденциальности и нормативным требованиям. Ключевые аспекты: • определение ролевой модели и прав доступа для пользователей; • управление и контроль доступа к данным; • удобство и скорость получения доступа; • мониторинг и аудит доступа к данным
Жизненный цикл данных	Цикл работы с данными, который включает процедуры создания/получения, передачи, преобразования и обработки, хранения, удаления/уничтожения данных
Зрелость системы управления данными	Степень, в которой организация последовательно и эффективно определяет, измеряет, контролирует и использует данные для достижения своих целей. Зрелая система управления данными характеризуется наличием хорошо определенных и функционирующих политик, процессов, стандартов и технологий для управления данными. Зрелость системы управления данными участника финансового рынка определяется на основе «Методики оценки зрелости систем управления данными участников финансового рынка» и «Опросника оценки уровня зрелости системы управления данными»

Золотая клиентская запись (Single Customer View)	Наиболее достоверное, непротиворечивое и полное представление о данных по клиенту организации. Является эталоном для сравнения, оценки и подтверждения информации из различных источников, что позволяет повысить качество данных и эффективность работы процессов организации
Интеграция данных	Управляемый процесс объединения данных из различных источников в согласованные физические или виртуальные формы, устраняющий дублирование и противоречия для ускорения бизнес-процессов и снижения затрат. Результатом процесса интеграции данных являются интегрированные данные – согласованные физические или виртуальные формы данных из различных источников, пригодные для анализа и принятия решений
Информационная система (ИТ-система)	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, которые дают возможность пользователям получать те или иные информационные сервисы для выполнения своих задач и функций
Инцидент качества данных	Зарегистрированный факт несоответствия данных требованиям к их качеству
Каталог проверок качества данных (реестр проверок качества данных)	Оформленная в виде каталога информация, содержащая сведения определяющие заказчика, принадлежность к данным, работу алгоритма проверки качества данных и взаимосвязи между проверками
Качество данных (Data Quality (DQ)	Состояние данных в ИТ-системах организации, при котором присущие данным характеристики отвечают требованиям организации и делают данные пригодными для анализа и использования
Концептуальная модель данных	Бизнес-описание сущностей и связей между ними, сгруппированных по предметным областям, без детализации до атрибутов
Корпоративная модель данных	Совокупность концептуальных моделей данных предметных областей, прикладных логических и физических моделей данных, а также описаний форматов обмена данными
КПЭ (KPI)	Ключевой показатель эффективности какой-либо деятельности – например, деятельности подразделения и/или организации
Критичные данные (Critical Data Elements (CDE)	Данные, имеющие ключевое значение для успешного функционирования основных бизнес-процессов организации
Логическая модель данных	Описание сущностей данных, детализированных до атрибутов и связей
Матрица RACI	Матрица ответственности – инструмент для управления отношениями в команде, который помогает избежать ситуаций, когда непонятно, кто какими задачами занимается. Аббревиатура RACI расшифровывается следующим образом: R (responsible) – исполнитель задачи или подзадачи проекта. Тот, кто самостоятельно выполняет все работы в рамках задачи. Если задача масштабная, у нее может быть несколько исполнителей. Однако эффективнее разбить ее на подзадачи и назначить исполнителей для каждой из них. A (accountable) – ответственный за всю задачу. Участник с этой ролью несет ответственность за то, чтобы задачу завершили в срок, но необязательно выполняет ее сам. Часто A-участники назначают задачи и подзадачи R-участникам. Важно, чтобы у одной задачи был только один ответственный. При этом сам ответственный может быть одновременно и исполнителем. C (consult) – эксперт, который консультирует команду по вопросам, находящимся в его компетенции. Он не выполняет задачу, но дает советы и рекомендации, которые помогают выполнить ее эффективнее. I (informed) – участник, который должен быть в курсе выполнения задачи или ее результатов. Результат задачи влияет на дальнейшую деятельность I-участников, поэтому им важно следить, что происходит
Метаданные	Данные, описывающие содержание или тип данных, жизненный цикл данных, состав атрибутов, связи между объектами и другую служебную информацию
Методика оценки зрелости системы управления данными	Структурированный подход для оценки текущего состояния практик управления данными организации по сравнению с признанными стандартами или лучшими практиками в отрасли. Методика обычно включает набор критериев или показателей, по которым оценивается организация, а также шкалу для измерения уровня зрелости
Монетизация данных (Data Monetization)	Процесс преобразования накопленных данных и информации в измеримую финансовую выгоду через прямые доходы от продажи или лицензирования данных (внешняя монетизация) либо через повышение эффективности бизнес-процессов, включая оптимизацию затрат, увеличение продаж и снижение рисков (внутренняя монетизация)
Неструктурированные данные	Данные, произвольные по форме, которые не имеют заранее определенной структуры
Нормативно-справочная информация (НСИ)	Информация о системе классификации и кодирования данных, представленная в форме унифицированных классификаторов, справочников, их описаний и применяемая для обеспечения единообразного формирования, представления, обработки и использования данных
Обеспечение качества данных	Включает определение, измерение, контроль и мероприятия по улучшению качества данных в соответствии с требованиями бизнеса, в том числе такие аспекты, как полнота, точность, согласованность, актуальность и пригодность данных для использования по назначению
Объект данных	Описание экземпляра некоторой сущности реального мира в виде логически связанных атрибутов. Объект данных хранится в информационной системе в виде, доступном для использования
Объекты управления СУД	Объектами управления системы управления данными являются: • объекты данных, которые участник финансового рынка использует и производит; • действия, выполняемые с объектами данных; • участники системы управления данными, выполняющие действия с объектами данных
Основные данные	Данные об объектах данных и бизнес-сущностях, представляющих ценность для организации

Первичные данные	Детальные данные, обычно развернутые до описания характеристик индивидуальных субъектов, объектов, операций
Политика управления данными	Документ, регламентирующий ключевые аспекты управления данными, описывающий цели и объекты управления данными, базовые термины, принципы и процессы управления данными, органы управления, роли участников в системе управления данными и их ответственность
Продвинутая аналитика (Advanced Analytics)	Технология автоматического либо полуавтоматического изучения данных и способа их интерпретации, работающая с большими массивами данных и позволяющая решать задачи поиска точек роста, идентифицировать тенденции, прогнозировать, оценивать вероятности потенциальных событий
Производные данные	Сводные данные и аналитические показатели, формируемые на основе первичных данных
Риск данных	Вероятность изменения свойств или характеристик качества данных, которые могут привести к прямым или непрямым потерям
Руководство данными	Деятельность по осуществлению руководящих и контрольных полномочий, а также по обеспечению совместного принятия решений (планирование, мониторинг и обеспечение выполнения) в отношении управления данными
Семантический слой данных (Semantic Data layer)	Слой архитектуры данных, формирующий поверх хранилищ и витрин данных единые определения показателей, сущностей и связей между ними, обеспечивающий пользователям согласованные представления и интерпретацию данных
Система управления данными (СУД)	Совокупность взаимосвязанных методологических, организационных и архитектурно-технологических компонентов, решающих задачи управления данными и включающих стандарты, политики, процедуры, правила и иные методологические документы
Слабоструктурированные данные	Данные, организованные в соответствии с определенными правилами и форматами, допускающими возможность произвольного представления информации, или произвольные по форме данные, которые не имеют заранее определенной структуры
Соглашение по обмену/об обмене данными	Формализованные между системами-источниками и ссистемами-потребителями условия, обязательства и технические параметры обмена данными. Форма, состав и детализация соглашения определяется потребностями сторон. Соглашение может включать спецификации интерфейсов (схемы, форматы, протоколы), требования к качеству данных и метаданным, параметры доступности, процедуры управления изменениями и распределение ответственности
Справочные данные	Унифицирующая информация и данные, применяемые для обеспечения единообразного формирования, представления, обработки и использования данных
Стандарты интеграции	Набор правил, протоколов и практик, которые определяют единообразность в способах обмена данными между различными информационными системами. Они обеспечивают совместимость, согласованность и эффективность передачи информации в гетерогенной ИТ-среде. Стандарты интеграции могут включать: • форматы данных (XML, JSON, CSV и другие); • протоколы передачи данных (HTTP, FTP, SMTP, SOAP, REST и другие); • модели данных и схемы (общие справочники и классификаторы и другие); • правила валидации, очистки и обогащения данных; • механизмы аутентификации, авторизации и шифрования; • шаблоны интеграционных процессов (ETL, ELT, CDC и другие)
Стратегия управления данными	Документ организации, включающий видение и миссию системы управления данными, долгосрочные цели и задачи, анализ текущего состояния, ключевые инициативы и проекты, дорожную карту реализации, необходимые ресурсы и бюджет, ключевые показатели эффективности, риски и стратегии их уменьшения, план коммуникаций
Структурированные данные	Данные, организованные и упорядоченные таким образом, чтобы обеспечить возможность применения к ним процедур обработки и преобразования в автоматизированных системах
Схема метаданных	Формальное структурированное описание типа информации, которая описывает данные (метаданные). Другими словами, это «чертеж», определяющий, какие атрибуты (элементы метаданных) используются для описания данных в определенном ракурсе
Транзакционные данные	Данные, описывающие действия, совершенные над основными данными
Управление качеством данных	Управление качеством данных включает контроль, мониторинг и улучшение характеристик данных, то есть установление стандартов и критериев качества данных (характеристик и метрик), валидацию и измерение характеристик данных, очистку данных, мониторинг и аудит качества данных, обратную связь и исправление ошибок при нарушениях качества данных
Управление метаданными	Планирование, реализация и контроль деятельности по обеспечению доступа к качественным, интегрированным метаданным, включая определения, модели, описания потоков данных и другую информацию, необходимую для понимания данных, а также систем, используемых для их создания, ведения и доступа к ним
Уровень зрелости системы управления данными	Подход к оценке степени развития системы управления данными организации на основе: • наличия и использования типовых организационно-распорядительных документов и методик работы с данными внутри организации; • наличия ценностей корпоративной культуры, ориентированных на работу с данными; • количества и состава ролей в процессах управления данными; • ресурсообеспеченности процессов управления данными; • наличия и использования специализированного программного обеспечения; • наличия и использования практик системы управления данными; • уровня дисциплины и качества предоставления регуляторной отчетности в Банк России. Определяется на основе «Методики оценки зрелости систем управления данными участников финансового рынка» и «Опросника оценки уровня зрелости системы управления данными»

Участники финансового рынка (УФР)	Организации, в отношении которых Банк России осуществляет регулирование и контроль (надзор) в соответствии с Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»
Физическая модель данных	Представление структуры данных, реализованной или предназначенной для реализации в системе управления базой данных. Отражает все свойства (атрибуты) информационных объектов базы данных и связи между ними с учетом способа их хранения в используемой системе управления базой данных
OLA, SLA	Соглашения между заказчиком и исполнителем о качестве оказываемых услуг. В соглашениях описываются параметры предоставления услуг: качество, количество, сроки, момент предоставления, время реакции и другие важные для заказчика параметры. Operational Level Agreement (OLA) – внутреннее соглашение в организации, определяющее зоны ответственности и параметры предоставления услуг между подразделениями. Service Level Agreement (SLA) – договор между заказчиком и поставщиком, содержащий описание услуги, права, обязанности сторон и штрафные санкции за нарушение условий предоставления услуг