ФБК

Аудит | Консалтинг | Право

Независимая оценка качества данных в информационных системах: регуляторные нормы и практики

Программа вебинара

1. Регуляторные требования к проведению независимой оценки качества данных в информационных системах: зачем, кто и когда должны производить оценку

2. Требования Положения Банка России №716-П к организации процесса управления качеством данных

3. Что такое данные в информационных системах и характеристики определяющие их качество

Спикер

Майя Савицкая

Менеджер,
Департамент аудиторских и консультационных услуг финансовым институтам

ФБК

Программа вебинара

4 **Важность качества данных**
- **примеры из разных отраслей и бизнес процессов;**
- **экономические последствия некачественных данных**

5 **Что должно быть в организации, чтоб провести оценку качества данных**

6 **Этапы оценки качества данных**

7 **Используемые российские и зарубежные стандарты**

Спикер

Рощупкин Иван

Ведущий эксперт по ИБ

ЭфБиКей Сайберсекьюрити

Регуляторные требования по проведению независимой оценки качества данных в информационных системах

Положение Банка России от 08.04.2020 №716-П

О требованиях к системе управления операционным риском в кредитной организации и банковской группе» пункт 8.7.6 главы 8 «Управление риском информационных систем

Во внутренних документах кредитной организации должен быть определен следующий порядок обеспечения качества данных в информационных системах, обеспечивающих критически важные процессы:

Порядок и периодичность (не реже одного раза в год) проведения независимой оценки качества данных в информационных системах

ПЕРИОДИЧНОСТЬ ОЦЕНКИ

Не реже одного раза в год

РЕГЛАМЕНТАЦИЯ

Порядок оценки регламентируется в ВНД КО

КТО ПРОВОДИТ

Оценка независимая

ПРЕДМЕТ ОЦЕНКИ

Данные в информационных системах, обеспечивающих **критически важные процессы**

ЧТО ОЦЕНИВАЕМ

Качество данных

“

Регламентация

”

Что закрепляется в ВНД

1. Порядок проведения оценки
2. Периодичность (не реже одного раза в год) проведения оценки
3. Уполномоченное подразделение, проводящее оценку
4. Правила и критерии привлечения внешних экспертов
5. Порядок принятия решения СД (НС) о проведении оценки

Обоснование

- п.4.1.1 Положения №716-П
- п.8.7.6 Положения №716-П
- Разъяснения БР от 23.10.2020 № 716-Р-2020/5
- Разъяснения БР от 17.05.2022 № 716-Р-2022/74

“

Информационная система

”

Федеральный закон от 27.07.2006 №149-ФЗ

Об информации, информационных технологиях и о защите информации

> **Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств**

ГОСТ 33707-2016 (ISO/IEC 2382:2015)

«Информационные технологии. Словарь»

> **Информационная система - система, организующая обработку информации о предметной области и ее хранение**

Положение Банка России №716-П:

ИНФОРМАЦИОННАЯ СИСТЕМА – ЭТО:

Технические и программные средства, поддерживающие и обеспечивающие непрерывность функционирования процессов кредитной организации (головной кредитной организации банковской группы)

Автоматизированные системы, программные и (или) программно-аппаратные средства, телекоммуникационное оборудование и линии связи (абз.12 п.4.1.5)

Критически важные процессы

Критически важные процессы – процессы, которые обеспечивают выполнение КО операций (пункт 4.1.1. Положения №716-П):

- Привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок)
- Размещение указанных в пункте 1 части первой настоящей статьи привлеченных средств от своего имени и за свой счет
- Осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам
- Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)
- Открытие и ведение банковских счетов физических и юридических лиц
- Ведение бухгалтерского учета
- Представление отчетности в банк России в соответствии с указанием БР № 4927-У
- Поддержание ликвидности
- Выполнение операций на финансовых рынках
- Выполнение кассовых операций
- Работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций
- Соблюдение требований федерального закона № 152-ФЗ "О персональных данных"
- Соблюдение требование трудового кодекса Российской Федерации
- **А также другие процессы, которые определены КО и прерывание функционирования которых оказывает влияние на выполнение обязательств перед клиентами и контрагентами КО**

“

Данные

”

ДАННЫЕ – ЭТО:

Представление информации в формализованном виде, пригодномдля передачи, интерпретации или обработки людьми или компьютерами
(ГОСТ 33707-2016 (ISO/IEC 2382:2015) «Информационные технологии. Словарь»)

Формы представления информации, с которыми имеют дело информационные системы и их пользователи
(ГОСТ Р ИСО/МЭК 10746-2-2000 «Информационная технология. Взаимосвязь открытых систем. Управление данными и открытая распределенная обработка»)

Качество данных

КАЧЕСТВО ДАННЫХ — характеристика, показывающая степень пригодности данных к использованию)

https://ru.wikipedia.org/wiki/Качество_данных

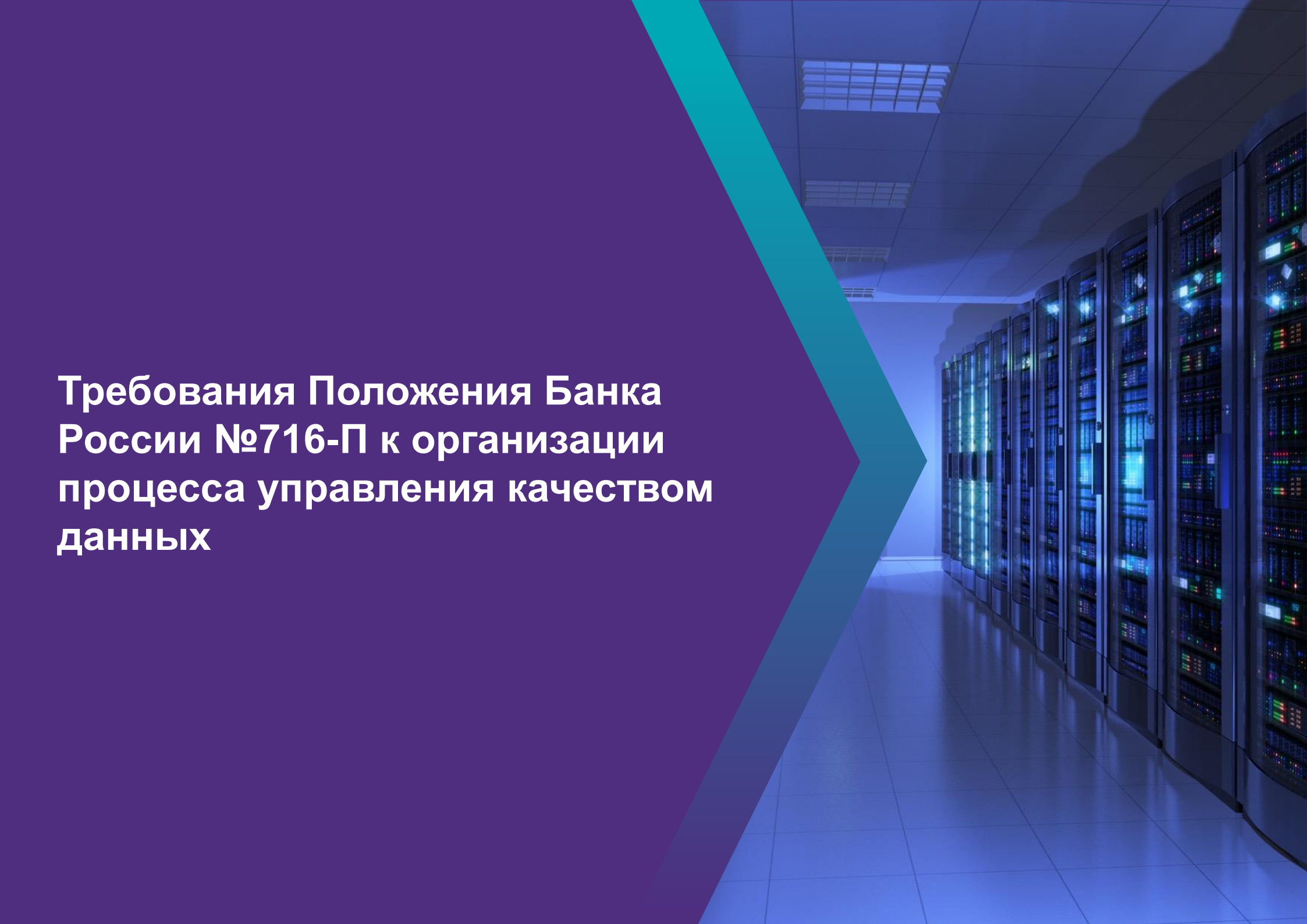
КАЧЕСТВО ДАННЫХ – степень, с которой **набор характеристик,** присущих данным, **отвечает требованиям**

Требование – потребность или ожидание которое установлено, предполагается или является обязательным

Несоответствие данных – невыполнение требований

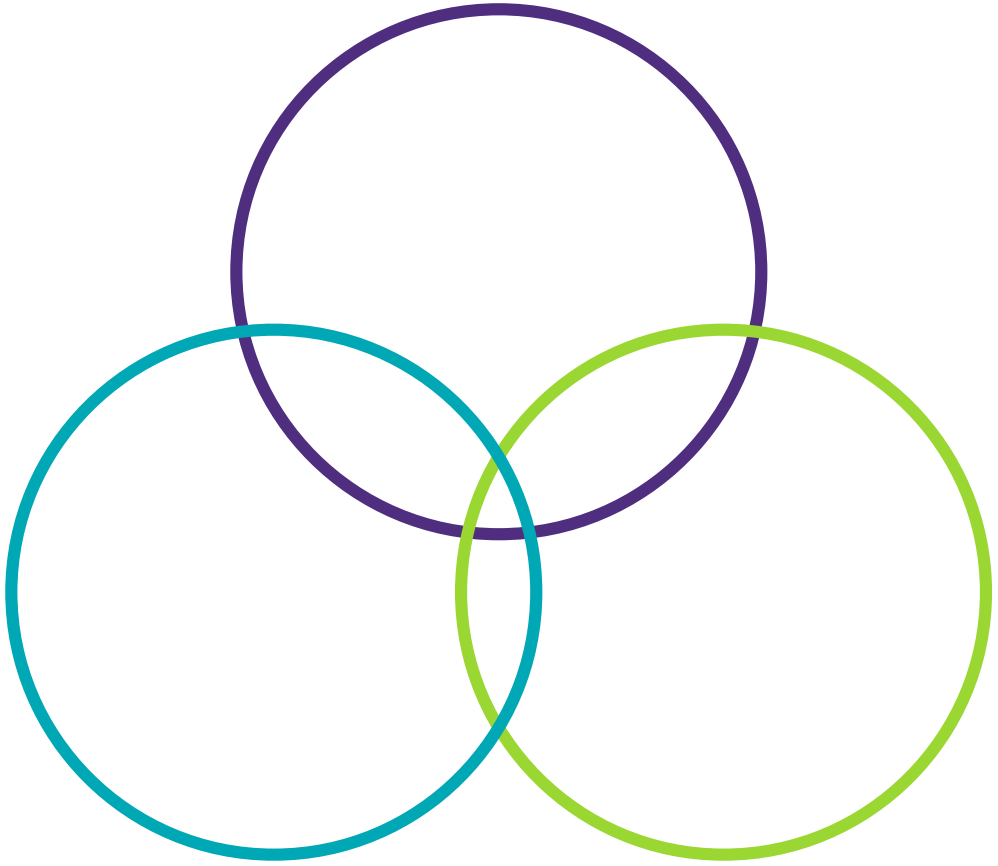
(ГОСТ Р ИСО 8000-2-2019 «Качество данных. Словарь»)

Требования Положения Банка России №716-П к организации процесса управления качеством данных



Требования к обеспечению качества данных в информационных системах, обеспечивающих критически важные процессы

(п.8.7.4 Положения №716-П)



- **Характеристики качества данных в ИС**
- **Порядок обеспечения качества данных в ИС**
- **Методика обеспечения качества данных в ИС**

Политика обеспечения качества данных в ИС
(п.8.7.6 Положения №716-П)

- **Процедуры** измерения показателей качества данных
- **Процедуры обоснования, утверждения и корректировки предельно допустимых значений показателей** качества данных, **критериев оценки** качества данных
- **Процедуры реагирования на случаи нарушения установленных КО предельно допустимых значений показателей** качества данных, критериев оценки качества данных
- **Процедуры, правила и периодичность контроля качества данных и формирования отчетов** о качестве данных, о проведении мероприятий контроля качества данных
- **Процедуры исправления выявленных ошибок в данных и документирования** внесенных в них изменений
- **Порядок взаимодействия** органов управления, подразделений и должностных лиц КО по вопросам обеспечения качества данных, устанавливающий их полномочия, ответственность, подотчетность и обеспеченность ресурсами, в том числе определяющий КО должностное лицо (должностные лица), несущее (несущие) персональную ответственность за обеспечение качества данных в ИС
- **Порядок и периодичность (не реже одного раза в год) проведения независимой оценки качества данных**
- Другие элементы порядка обеспечения качества данных в ИС

Методика обеспечения качества данных в ИС (п.8.7.5 Положения №716-П)

- **Классификатор** возможных **источников и причин образования** в ИС **данных**, **не соответствующих требованиям** к качеству данных в ИС
- **Показатели (индикаторы) качества данных для оценки характеристик качества данных**, разрабатываемые КО **для различных информационных систем**
- **Методы и алгоритмы расчета, правила измерения** показателей качества данных, в том числе **с использованием контрольных выборок данных**
- **Критерии оценки** качества данных
- Другие элементы методики обеспечения качества данных в ИС

Элементы Методики применяются с учетом особенностей конкретных данных, в том числе методов и процедур их фиксирования, хранения и преобразования, а также их типов и форматов

Характеристики качества данных (1)
(п.8.7.4 Положения №716-П)

- Точность и достоверность
- Полнота
- Актуальность данных
- Согласованность
- Доступность
- Контролируемость
- Восстанавливаемость

Характеристики качества данных (2)
(п.8.7.4 Положения №716-П)

Другие характеристики качества данных определяются КО самостоятельно с учетом

Осуществляемых операций

Текущих и стратегических планов развития

Действующих процессов

Доступных возможностей

Уровня и сочетания принимаемых рисков

Характеристики качества данных закрепляются в ВНД

Точность и достоверность данных

1

Что это значит?

Это отсутствие синтаксических и семантических ошибок в данных, а также их соответствия реальным и статистически наиболее вероятным значениям свойств, характеристик и параметров, зафиксированных в данных

Как это оценить?

Для оценки могут использоваться частные показатели:

- Корректность записей (доля значений, несоответствующих корректным), выявленных по результатам обработки инцидентов, связанных с качеством данных
- Соответствие эталонным данным/первоисточникам

Полнота данных

2

Что это значит?

Это достаточность данных для обеспечения функционирования банковских процессов

Как это оценить?

Для оценки могут использоваться частные показатели:

- Доля незаполненных полей (атрибутов) обязательных к заполнению
- Доля объектов учета, данные о которых включены в ИС, в общей массе объектов учета
- Доля записей с избыточными (например, полученными в результате дублирования) значениями

Актуальность данных

3

Что это значит?

Это свойство данных адекватно отражать состояние объектов предметной области в текущий момент времени

Как это оценить?

Для оценки могут использоваться частные показатели:

- Доля актуальных данных в составе ИС (массива данных).
- Коэффициент готовности данных (отношение времени пребывания в актуальном/нормативном состоянии к времени пребывания в неактуальном или неопределенном состоянии).
- Коэффициент длительности обработки, проверки ошибок, согласования и внесения данных в информационной системе.

Согласованность данных

4

Что это значит?

Это свойство данных в любой момент времени адекватно отражать состояние объектов взаимной непротиворечивости данных, хранящихся в ИС, других источниках и носителях информации

Как это оценить?

Для оценки могут использоваться частные показатели:

- Доля использования альтернативного обозначения или сокращения для сущностей, снабженных стандартизованным обозначением
- Доля нестандартных наименований объектов учета

Доступность данных

5

Что это значит?

Это возможность использования данных при функционировании процессов

Как это оценить?

Для оценки могут использоваться частные показатели:

- Время доступности
- Время простоя ИС

Контролируемость данных

6

Что это значит?

Это возможность осуществления контроля качества и происхождения данных

Как это оценить?

Для оценки могут использоваться частные показатели:

Характеристика оценивается наличием в ИС следующего функционала отражения:

- источников данных;
- истории создания;
- истории изменения;
- истории преобразования;
- истории удаления;
- истории хранения;
- истории передачи данных

Восстанавливаемость данных

7

Что это такое?

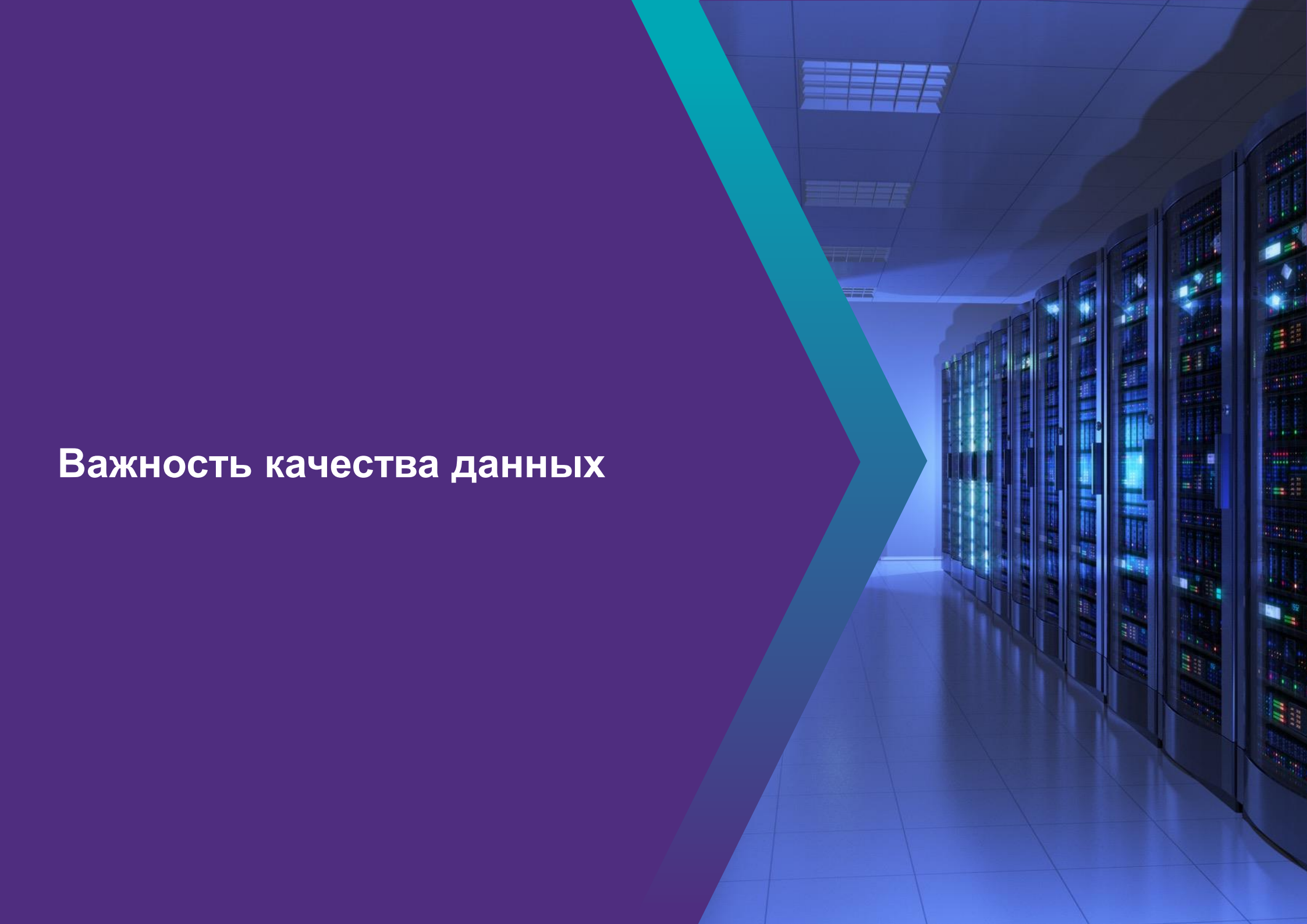
Это возможность сохранять установленный уровень функциональности и качества данных после их утраты, повреждения или изменения в результате сбоев или других нарушений функционирования информационных систем

Как это оценить?

Для оценки могут использоваться частные показатели:

- RPO (Recovery point objective) - целевая точка восстановления. Целевая точка восстановления (RPO) определяется допускаемым уровнем потери данных в случае прерывания операций.

Важность качества данных



Примеры из разных отраслей и бизнес процессов

Качества данных в государственных системах

1. В реестре субсидий Федерального казначейства присутствуют записи, в которых сумма по соглашению получателя субсидии расходится с фактическими суммами по платёжным поручениям

2. В ноябрь 2020 года в открытых данных **ФНС** содержались сведения о 39 000 предприятиях, прекративших деятельность раньше, чем они были зарегистрированы. Есть записи, где на один ИНН приходится несколько десятков предприятий, а, по открытым данным **московского правительства**, в городе числятся дома, площадь которых превышает 4 млн кв. м. и жильё площадью всего 1 м^2.).

из материалов www.osp.ru

ПРИЧИНА: Отсутствие автоматического контроля механизма сверки сумм соглашений и платежных поручений

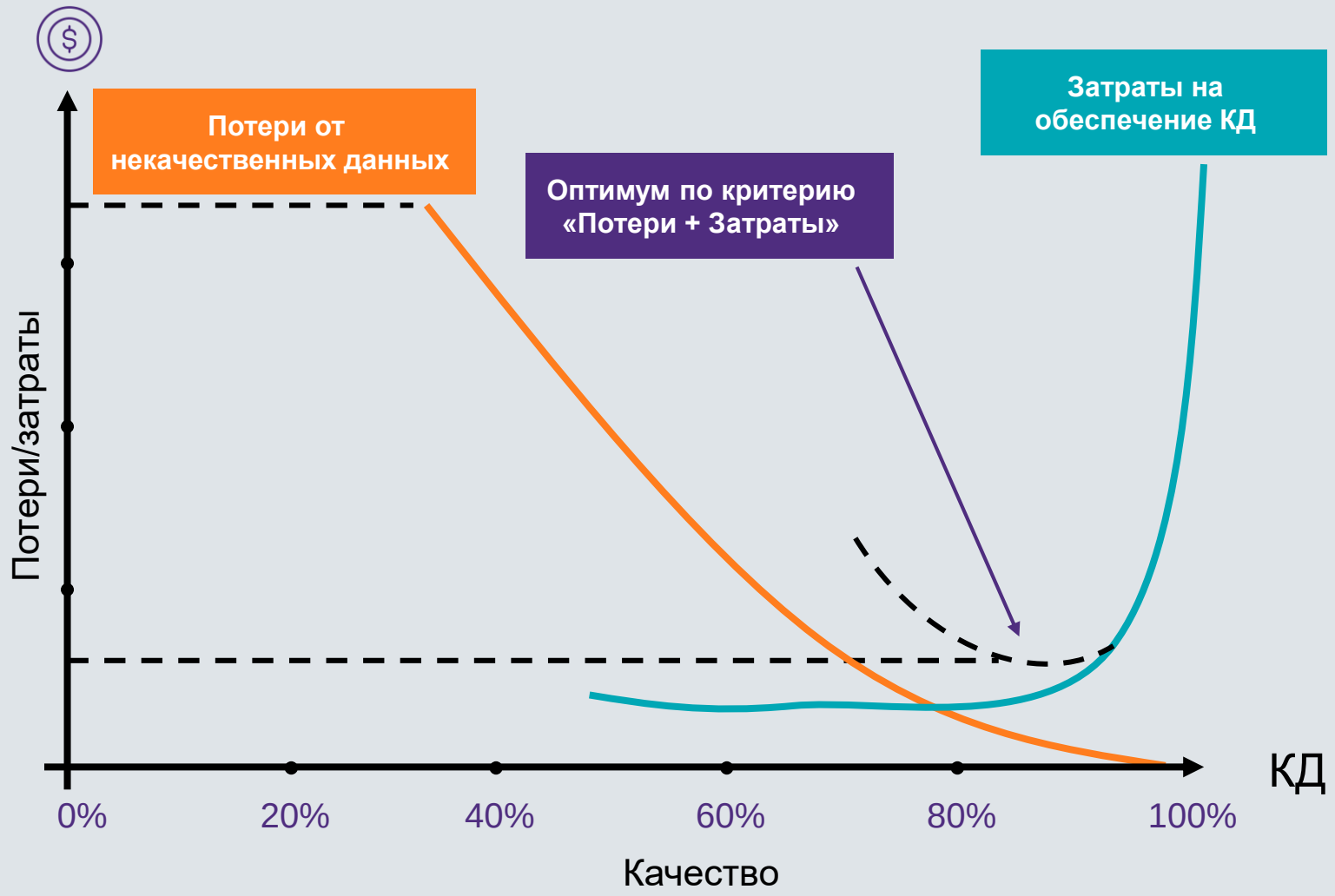
Важность качества данных в проектах

3 Ошибка в огромном заказе от французских железных дорог SNCF на 2 тыс. поездов в 2014 году.

4 Дорогой ошибкой, вызванной неправильными исходными данными, считается авария ракеты Ариан-5.

Экономические последствия некачественных данных

Экономика качества данных в теории



Статистика по потерям

Из-за низкого качества информации:

83% **Фирм терпят финансовые убытки**

15% **Процент убытка от реальных доходов компании**

Плохое качество используемых данных отрицательно влияет на продуктивность работы различных компаний:

20% **Сокращение производительности**

Результаты исследований:

> от **15 до 35%** годового бюджета организации тратится неэффективно из-за низкого качества данных. Причем в организациях, ориентированных на предоставление услуг (таких как банки, страховые компании, правительственные учреждения), объем **потерь доходит до 40%**

Источник https://imccenter.ru

Экономические потери

Бюджетные потери на выполнения некачественной услуги

Цена ошибки — модернизация всей инфраструктуры на сотни миллионов евро

Потеря доверия к поставщику услуги

Суммарный урон по итогу этого случая оценивают в 0.5 миллиардов долларов в ценах начала 1996 года

Источник https://habr.com

Что должно быть в организации, чтобы провести оценку качества данных

Требования к функционированию существующих процессов в организации

№	Высокоуровневые требования для ИТ- систем
1	Описание ИТ-архитектуры
2	Методическое обеспечение процессов ИТ и описание
3	Описание процессов поддержки ИТ-систем

№	Высокоуровневые требования для процессов ИТ
1	Процессы управления изменениями
2	Описание информационного пространства пользователей
3	Управление ответственностью и процессами согласования

Проведение организацией мероприятий по выполнению требований 716-П

Общие требования для обеспечения качества данных

1. Документальное описание процесса обеспечения качества в ИТ-системах
2. Документальное описание ИТ-систем по обеспечению качества данных
3. Стандартизация и описание данных в организации
4. Описание процедур управления интеграционным взаимодействием
5. Выполнение и описание контроля межсистемной целостности данных
6. Управление ответственностью и процессами согласования
7. Регулярная модернизация и усовершенствование качества данных параллельно развитию бизнес-процессов организации
8. Проверки и мониторинг данных
9. Классификация возможных источников и причин образования некачественных данных в ИС

Этапы оценки качества данных

Пример Этапов оценки качества данных в Организации

Анализ Организации для дательной оценки КД

Изучаются процессы и процедуры, структура Организации для дательной оценки качества данных :

- Изучение ВНД, регламентирующих систему управления риском информационных систем и процедуры управления качеством данных в ИС;
- Проведение интервью с работниками, участвующими в процессах и процедурах управления риском ИБ и риском ИС;
- Тестирование на выборочной основе реализации отдельных процедур по управлению качеством данных, регламентированных в ВНД;
- Выделение и проверка критических процессов в организации и относящийся к ним ИС;
- Определение степени зрелости системы управления, методики и процедур Банка в сфере обеспечения качества данных;
- Определение СУБД и перечень данных для оценки;
- Составление каталога данных с описанием требуемых атрибутов для оценки качества данных;
- Модели ИС, бизнес процессы, данных.

Изучаются процессы и процедуры ИТ

- Ит-архитектура;
- Методическое обеспечение процессов ИТ;
- Процессы обеспечения качества в ИТ-системах;
- Функциональность ИТ-систем по обеспечению качества данных;
- Процессы поддержки ИТ-систем;
- Процессы управления изменениями;
- Информационное пространство пользователей;
- Описание данных (стандартизация);
- Профилирование и мониторинг данных;
- Управление интеграционным взаимодействием;
- Контроль межсистемной целостности данных;
- Управление ответственностью и процессам согласования;
- Модернизация и усовершенствование качества данных параллельно развитию бизнес-процессов банка;
- Классификатор возможных источников и причин образования некачественных данных в ИС;

Что делают специалисты при внешней оценке

- Проводят Gap-анализ ВНД Банка и проводимых в соответствии с ними процедур на предмет соответствия требованиям п.8.7.4 - 8.7.6 8 Главы Положения №716-П;
- В случае выявления фактов несоответствия предложат Банку рекомендации по проведению мероприятий, направленных на минимизацию регуляторного риска и риска ИС;
- Проводят оценку соответствия процедур по управлению качеством данных в ИС с использованием стандарта оценки Банка России;
- Помогут выделить критические процессы в организации и относящиеся к ним ИС организации;
- Определяют степени зрелости системы управления, методики и процедуры Банка в сфере обеспечения качества данных;
- Определяют СУБД и перечень данных для оценки;
- Составляют каталоги данных с описанием требуемых атрибутов для оценки качества данных.

Результаты работы внешнего оценщика

При завершении работы организация получает:

- Вывод по оценке процедур управления качеством данных в ИС с использованием шкалы Банка России
- Рекомендации, направленные на повышение эффективности системы управления риском ИС в части управления качеством данных в ИС а также для повышения уровня ее соответствия требованиям Положения Банка Росси №716-П
- Описание критических процессов и ИС
- Оценка степени зрелости системы управления, методики и процедур организации в сфере обеспечения качества данных
- Каталог данных с описанием требуемых атрибутов для оценки качества данных
- Модель ИС, бизнес процессов, данных

Возможные источники угрозы образования в ИС данных, не соответствующих требованиям к качеству данных

№	Источник угрозы	Описание
1	**Ошибка персонала**	Любые не соответствующие установленным регламентам или сложившимся практикам действия персонала, совершаемые без злого умысла по причине недостаточно четко определенных обязанностей, недостаточного обучения или квалификации персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, отсутствие методов контроля, предоставление избыточных полномочий и др.
2	**Социальный инжиниринг**	Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение персонала, приводящие к ошибкам работников, несанкционированным изменениям и утрате информационных активов, нарушению конфиденциальности данных.
3	**Несанкционированный логический доступ**	Несанкционированный логический доступ неавторизованных субъектов к информационным активам (компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств, вредоносные программы) может привести к нарушению свойств информационных активов, к сбоям, отказам, несанкционированным изменениям и уничтожению программных средств и информации.

№	Источник угрозы	Описание
4	**Несанкционированный физический доступ**	Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или информационных активов, что может привести к разрушению и уничтожению технических и программных средств, нарушению конфиденциальности, целостности, доступности информационных активов, нарушению непрерывности процессов.
5	**Выполнение вредоносных программ**	Внедрение в систему и выполнение вредоносных программ вследствие халатности, низкой квалификации персонала (пользователей), наличия уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, информации.
6	**Использование программных средств и информации без гарантии источника**	Использование в информационной системе организации непроверенных данных или нелицензионного программного обеспечения.
7	**Нарушения договорных обязательств сторонними (третьими) лицами**	Невыполнение со стороны третьих лиц взятых на себя обязательств по качеству, составу, содержанию и/или порядку оказания услуг, поставки программно-технических средств и т.д.

№	Источник угрозы	Описание
8	**Ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла**	Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем.
9	**Сбои и отказы программно-технических средств**	Нарушение работоспособности программно-технических средств, технические сбои, в том числе неполная загрузка данных, некорректная логика преобразований данных вследствие некорректного изменения параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий.
10	**Нарушения функциональности криптографической системы**	Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно--аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности данных, нарушению бесперебойности приема-передачи информации, блокировке функционирования информационных систем.
11	**Нарушения функциональности архивной системы**	Нарушение конфиденциальности и целостности архивных данных и/или непредоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы.

Пример с 483-П

Требования к качеству данных, используемых банками для создания и применения моделей количественной оценки кредитного риска для целей расчета нормативов достаточности капитала

Расчёт кредитного риска по 483-П (ПВР)

В качестве примера приведен расчет параметров риска для кредитного требования к финансовой организации:

Объём	**100 млн руб.**
Срок	**5 лет**
Уровень потерь при дефолте	**45%**
Вероятность дефолта	**5% (PD = 0,05)**
Величина ожидаемых потерь	**2,25 млн руб**
Величина кредитного риска	**31,512 млн руб**
Поправочный коэффициент	**1,06**

Для корпоративного, суверенного заемщика и финансовых организаций, по которым не произошел дефолт PD ≠ 100%

Результаты расчётов:

КРП = 190,491
EL = 2,250
UL = 14,377

Промежуточные результаты расчётов:

Кпвр = 1,797088
R = 0,129850
b(PD) = 0,079878

Расчёт кредитного риска по 483-П (ПВР)

Но при 2,5% наличии некачественных данных, возможно отклонение параметра потерь при дефолте 42%

Для кредитного требования к финансовой организации

Объём	**100 млн руб.**
Срок	**5 лет**
Уровень потерь при дефолте	**42%**
Вероятность дефолта	**5% (PD = 0,05)**
Величина ожидаемых потерь	**2,25 млн руб**
Величина кредитного риска	**31,512 млн руб**
Поправочный коэффициент	**1,06**

Для корпоративного, суверенного заемщика и финансовых организаций, по которым не произошел дефолт PD ≠ 100 %

Результаты расчётов:

КРП = 177,792 - как поменялись ?
EL = 2,100 - как поменялись ?
UL = 13,418

Промежуточные результаты расчётов:

Кпвр = 1,677282
R = 0,129850
b(PD) = 0,079878

Показатели при дефолте 45%

КРП = 190,491
EL = 2,250

КРП — величина кредитного риска
EL — (expected losses) величина ожидаемых потерь (убытков)

Используемые российские и зарубежные стандарты

№	Стандарты	Описание
1	**ISO/TS 8000 «Качество данных» (ГОСТ Р 56214-2014/ISO/TS 8000-1:2011)**	Стандарты комплекса ИСО 8000 определяют параметры характеристик, которые могут быть проверены любой организацией в цепочке передачи данных с целью определения соответствия этой информации требованиям ИСО 8000. Стандарты комплекса ИСО 8000 обеспечивают совершенствование качества информации, используемой как самостоятельно, так и в рамках систем управления качеством. В стандартах комплекса ИСО 8000 представлены технические характеристики качества данных, применяемых на протяжении всего жизненного цикла продукции, и рассматриваются различные виды данных, включая основные данные, данные транзакций и данные о продукции.
2	**ISO/IEC 25012:2008 Разработка программного обеспечения — Требования и оценка качества программного продукта (SQuaRE) — Модель качества данных**	SO/IEC 25012:2008 определяет общую модель качества данных для данных, хранящихся в структриро-ванном формате в компьютерной системе. 
3	**Документы Банка России по управлению качеством данных**	Письмо Банка России от 27.05.2014 № 96-Т Положение Банка России от 06.08.2015 № 483-П Прилож. №3 Положение Банка России от 08.04.2020 г. № 716-П

Выводы

Основные выводы

1. **Сложный относительно новый для большинства организаций процесс, который требует привлечение квалицированных специалистов в этой области.**

2. **Существующая методика и порядок обеспечения качества данных в информационных системах должны быть взаимоувязаны с другими процессами ИТ/**

3. **Повышение качества данных реально приносят выгоду для организации.**

ФБК

Аудит | Консалтинг | Право

Спасибо за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

T: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

fbk.ru

fbk-pravo.ru

fbkcs.ru