

# Особенности работы с бизнес-информацией

Введение в системный анализ



# Оглавление

<b>Введение</b>	<b>2</b>
<b>Термины, используемые в лекции</b>	<b>2</b>
<b>Понятие информации</b>	<b>3</b>
<b>Свойства информации</b>	<b>5</b>
<b>Особенности использования бизнес информации</b>	<b>14</b>
<b>Управление данными</b>	<b>20</b>
<b>Заключение</b>	<b>25</b>
<b>Что можно почитать еще?</b>	<b>26</b>
<b>Используемая литература</b>	<b>26</b>

## Введение

Мы продолжаем обучение по программе технической специализации системный анализ. На прошлом занятии мы ознакомились с понятием системы и системного подхода узнали какими бывают системы, ознакомились с инструментарием системного аналитика. Изучили и попрактиковались в приемах системного анализа.

Сегодня лекция будет направлена на развитие предыдущей темы и закрепление основ, используемых в системном анализе.

На лекции мы вспомним понятие информации, узнаем какими качествами обладает информация и какие особенности присущи процессу обработки информации в бизнес системах. Также мы поговорим о методах работы с данными.

# Термины, используемые в лекции

**Информация** – это любые сведения прямо или косвенно влияющие на состояние системы.

**Входная информация** – это абстракция всех ресурсов потребляемых системой, а также мера воздействия среды или обратной связи управления.

**Выходная информация** – это абстракция результат работы системы.

**Внутренняя (внутрисистемная) информация** – это тип информации который сохраняется в системе и отражает её состояние.

**Полнота** – свойство информации определяющее степень достаточности данных для принятия решения.

**Адекватность** – это мера соответствия информации действительности.

**Актуальность** – это свойство информации показывающее степень сохранения ценности в момент применения.

**Доступность** – это степень возможности воспринимать информацию со стороны потребителя.

**Достоверность** – показатель качества информации, свидетельствующий, что информация не искажает истинного положения дел.

**Бизнес информация** – это любые сведения характеризующие экономические объекты и их отношения используемая в процессе деятельности и управления.

**Репозиторий** – место где хранятся и обрабатываются данные.

# Понятие информации

Если представить систему в виде чёрного ящика, то на вход в системы подаются воздействия или ресурсы, на выходе результат. А сама система находится в среде. В общей информационной модели системы вход и выход представлены исключительно информацией. Взаимодействие со средой происходит так же лишь информационно.

Систему можно назвать управляемой если существует обратный информационный поток от результата к системе или к информационным ресурсам, прямо или косвенно на них воздействующий.

Возьмём для примера одну из самых простых и понятных систем — автомобиль. Педаль акселератора автомобиля вне зависимости от реализации сообщает системе двигателя с каким ресурсом ему предстоит работать в тот или иной момент времени. Результатом работы двигателя является момент вращения передаваемый на колеса автомобиля.

Таким образом, входной поток потребляемого топлива является управляемым прямо или косвенно и приводит к ожидаемому результату: автомобиль набирает скорость, и соблюдая правила дорожного движения едет по маршруту. Чем больше давление на педаль, тем выше крутящий момент и больше скорость.

Говоря о модели транспортного средства, мы можем абстрагироваться, то есть проигнорировать, определенную реализацию двигателя и вид используемого топлива. Упрощенная принципиальная модель системы в этом случае будет содержать лишь потоки информации виде угла наклона педали, объем ресурса — топлива или электроэнергии в единицу времени с одной стороны, и выходное значение крутящего момента или скорость с другой.



Проще говоря, этот пример показывает, что только информация имеет значение для модели системы, а следовательно и для системного анализа.

Давайте вместе ещё раз вспомним что такое информация и какими качествами она обладает. В приложении к системному анализу можно сказать что информация это сведения прямо или косвенно влияющие на состояние системы.

Относительно системы информацию можно разделить на 3 типа:

- входная,
- выходная,
- внутренняя.

**Входной** информации является абстракции всех ресурсов потребляемых системой, воздействием среды или обратной связи.

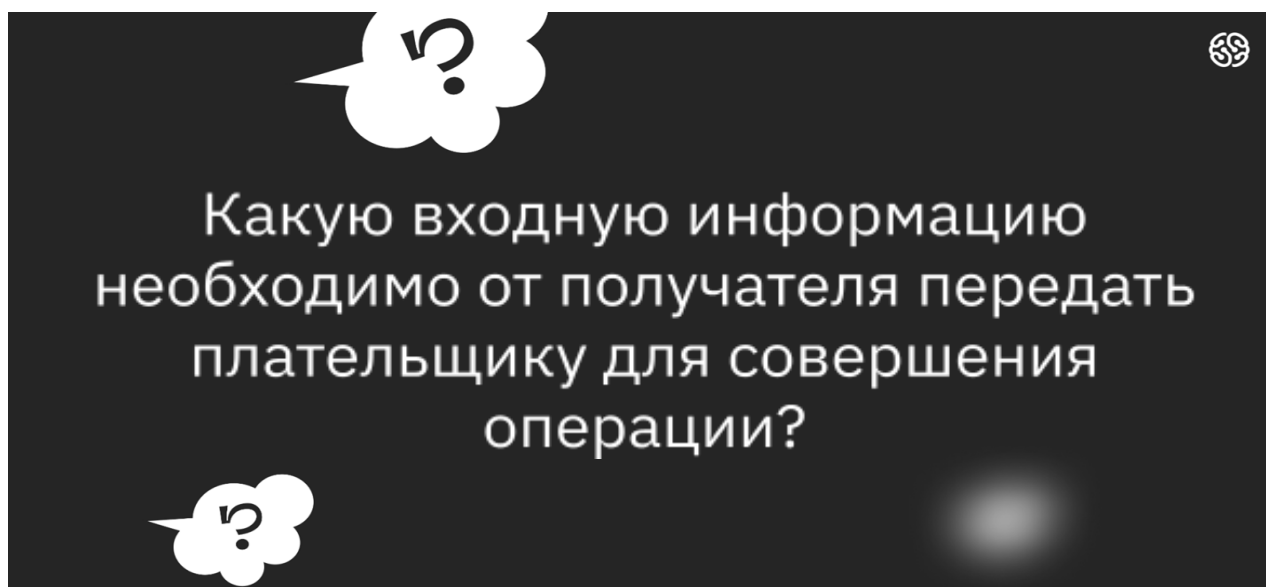
**Выходная** информация представляет собой результат работы системы.

**Внутренняя** или внутрисистемная информация – это тот тип информации который сохраняется в системе.

Например, банк осуществляющий перечисление денежных средств действует на основании распоряжения клиента. В качестве обратной связи зачастую выступает информация о результате проведения операции, а выходной информацией зачисленная сумма.



Возможно вам кажется этот пример слишком абстрактным, но что будет, если это вы ожидаете оплату на свой счёт. Подумайте, какую входную информацию вам необходимо передать плательщику, для того чтобы он зачислил ожидаемую вами сумму на ваш счёт?



**Ответ:** Уверен, вы справились заданием, назвав номер телефона при перечислении через систему быстрых платежей или набор реквизитов при перечислении на счёт или на карту. В номере сложно ошибиться, другая ситуация с реквизитами счёта.

## Свойства информации

Обычно реквизиты для перечисления представлены номером счёта (не стоит путать с 16-значным номером карты, который находится на лицевой стороне), банковским идентификационным кодом, номером корреспондентского счёта, КПП, ИНН, ОКПО, ОГРН, наименованием филиала, выдавшего платёжный инструмент, и его адресом.

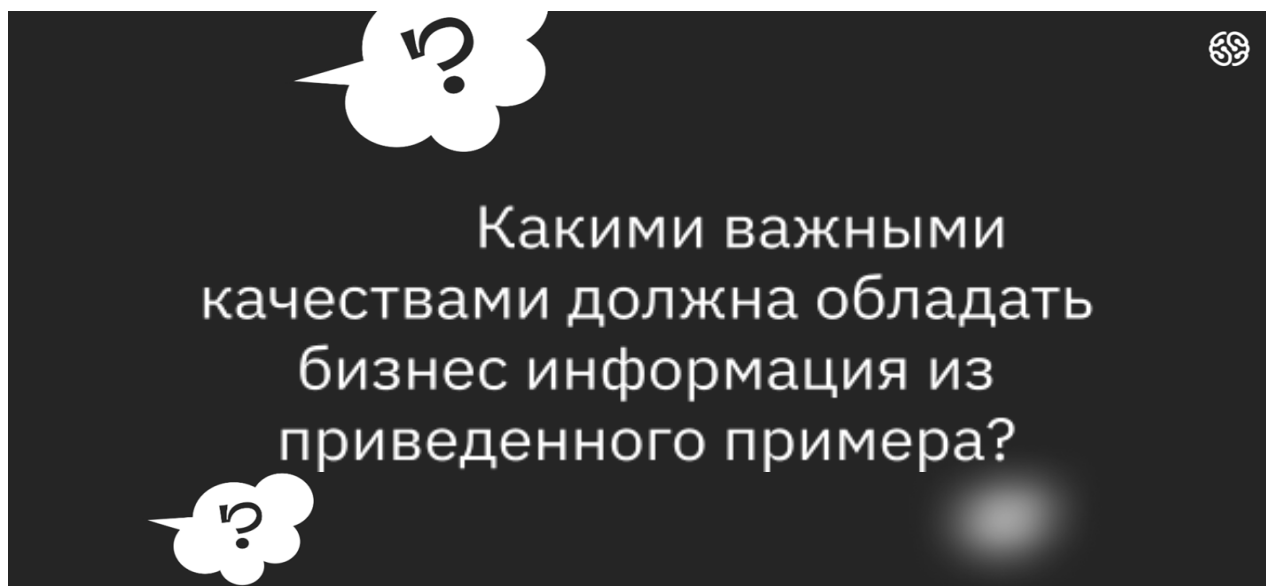
Само же платёжное поручение включает дополнительно сумму и назначение платежа.

Обилие требуемой информации для выполнения операций в платёжной системе вводит в замешательство любого неподготовленного человека. И например, если вы оформляете налоговый вычет и ошиблись в счёте перечисления, то платёж может быть отложен более чем на месяц.

Не стану вдаваться в детали, но ошибки при тех же операциях при таможенном оформлении экспорта и импорта могут иметь последствия в виде штрафа или тюремного заключения. Ошибки при сертификации товара – отзывом целой партии товара с рынка.

Давайте рассмотрим качества информации влияющие на результат. Как мы говорили выше, положительным результатом будем считать зачисление денежных средств без задержек по корректным реквизитам.

Подумайте, какими важными качествами должны обладать приведенные в примере сведения о реквизитах для перечисления денежных средств?



**Ответ:** Для бизнес-информации характерны те же свойства, что и для обычной информации, прежде всего это полнота.

Первое и самое важное свойство, это **полнота** или достаточность информации. Как мы выяснили ранее системе присуща цель. Так как мы рассматриваем платёжную систему, её цель заключается в перечислении денежных средств от плательщика к получателю. Не имея полной информации в реквизитах счёта получателя плательщика будет крайне сложно перечислить денежные средства, ну куда сложнее будет банку понять кому предназначаются средства зачислены, допустим не на лицевой персональный счёт, а на общий расчётный, без указания адресата. Полнота информации это такое свойство или качество информации, позволяющие системе принять решение соответствующее своей цели.

Если говорить о полноте информации, то наряду с недостатком информации ухудшить качество может ее избыток. Избыток информации затрудняет выделение необходимой для системы информации. Это легко проиллюстрировать, если бы в платёжном поручении нашего примера были указаны пять фамилий получателей и один номер коллективного счета.

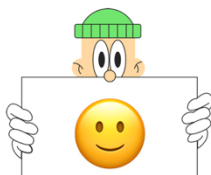
Смотрите, если бы информации было бы меньше, И платёжные поручения содержало бы номер коллективного счета и фамилию имя отчество получателя

средств тут такой информации было бы достаточно, увеличив объем информации добавив новые фамилии, одновременно увеличилась и неопределённость, ведь непонятно в какой пропорции между получателями необходимо распределить денежные средства.



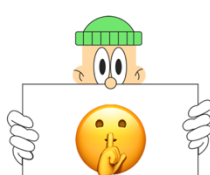
**Полнота информации  
позволяет системе принять  
решение**

Система принимает решение в соответствии со своей целью при достаточности информации



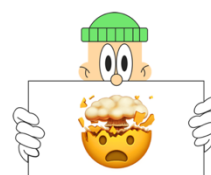
**Недостаток информации  
снижает возможность принять  
решение**

Например, при недостатке платежных реквизитов, платеж не сможет быть осуществлен



**Избыток информации так же  
снижает возможность принять  
решение**

Например, при избытке платежных реквизитов платеж может быть осуществлен по неверным реквизитам



На иллюстрации избыточности сведений можно подобрать другой пример, который очень часто встречается в практике. Допустим в платёжном поручении указана счетов больше чем нужно: корреспондентский счёт банка, расчётный счёт организации, лицевой счёт клиента, счёт для процентов и так далее. Получается, что в данном примере качество полноты информации выполняется, но системе будет сложно какой из перечисленных счетов принять к исполнению, а следовательно это повышает неопределённость.

Таким образом полнота информации это важнейшее качество для информационной системы, предусматривающие её достаточность для использования в рамках конкретной цели, но не избыточность.

Ещё пример. Допустим, в нашем платежном поручении присутствует коллективный карточный счёт и две персоналии первая фамилия Иванов Иван Иванович – получатель платежа, второй – ответственный за контроль перечисления. Ответственный за контроль Петров Пётр Петрович– это внутренние функции плательщика, некая должностное лицо осуществляющие входной контроль документов, и в принципе эта информация не должна передаваться в платёжном поручении, и с точки зрения перечисления денежных средств она не является необходимой.



Теперь представьте себе несовершенство банковской автоматизированной системы, когда с одной стороны, информация, направленная в банк, не бракуется на входном контроле. А с другой, внутренний дефект обработки, кстати очень распространённый, что из списка обнаруженных фамилий в платёжном поручении, для перечисления выбирается только одна, первая или последняя.

Так излишняя информация, встретившись с дефектом обработки на стороне банка, может привести к некорректному результату. В этом примере, в случае стечения вышеописанных обстоятельств, Пётр Петрович получит неожиданный платёж, и будет радоваться премии, правда не долго, в то время как Иван Иванович не получит ничего, до момента юридического отката транзакции, что может занять длительное время. Избыточная информация наряду с недостаточной могут влиять на работу системы и привести к ошибочному результату.

Информация – это как соль в рецепте: плохо когда её мало, и приходится собирать по крупицам, но ещё хуже когда её так много, что невозможно обработать. Раздел ИТ технологий позволяющий обрабатывать сколь угодно большие объёмы информации называется BigData, но стоимость такой обработки весьма высокая, что может привести к нерентабельности работы с информацией и её непригодности для цели системы.

**Адекватность** информации – это следующая характеристика, которая имеет ключевое значение при определении качества информации. Адекватность это мера соответствия информации действительности. Следует отметить что она бывает трёх типов, и все они важны для получения корректного результата, они в совокупности определяют качество информации.



#### **Синтаксическая адекватность**

Формальное представление соответствует объекту, например корректно указан номер банковского счета по шаблону 20 символов



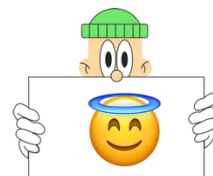
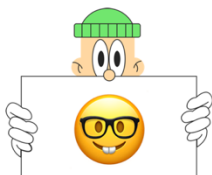
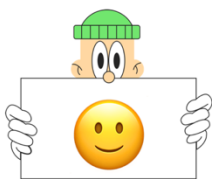
#### **Семантическая адекватность**

Смысловое представление соответствует объекту, например верно указан номер лицевого счета, а не корреспондентского



#### **Прагматическая адекватность**

Информация соответствует цели её использования, указаны реквизиты получателя, а не стороннего лица

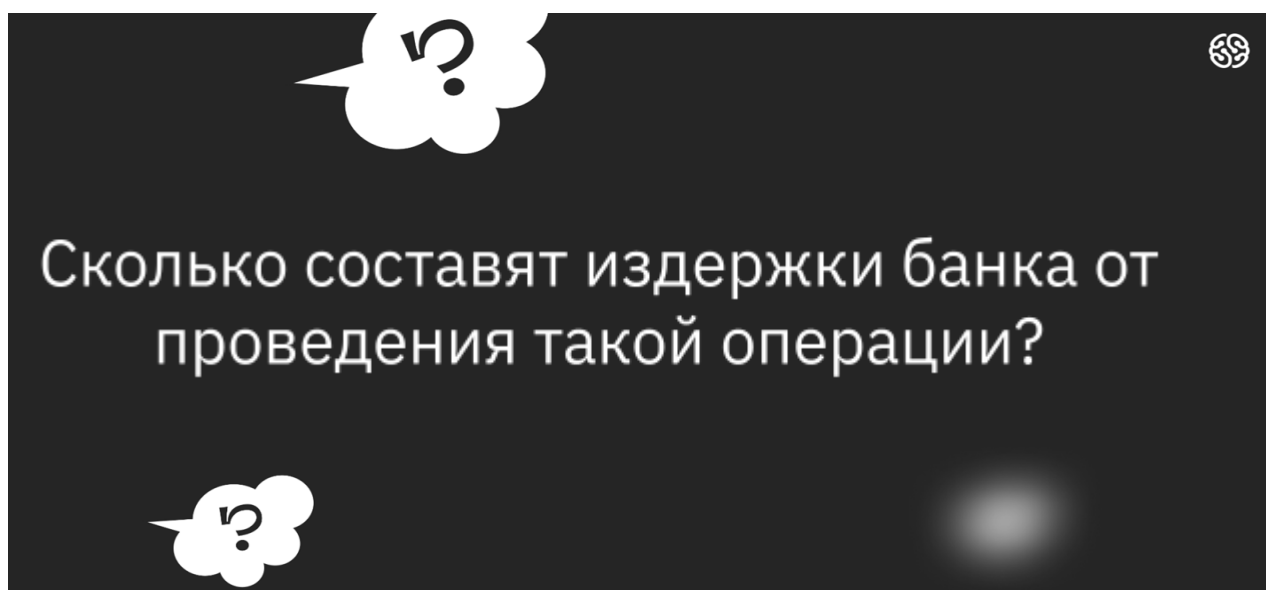


Рассмотрим первый тип адекватности — синтаксическую адекватность информации. Этот тип предусматривает, что для качественного представления информации, её формальное представление должно соответствовать объекту.

Например, значительное число белорусских фамилий и имён содержит буквы «а» вместо «о», таким образом возникает дуализм или двойное написание. Если в предыдущем примере перечисление денежных средств будет вестись с контролем имени, то гражданин республики Беларусь Раман (через а), рискует не получить перевод в России, а россиянин Роман в Беларуси.

Другой пример можно привести если рассмотреть кодировку чисел. Сумма платежа в рублёвой зоне выражается целым числом рублей, и дробной частью копеек. Если к примеру плательщик закодирует это число другой формой, допустим в двоичном формате, то получатель получит другую сумму.

Постарайтесь сосчитать сколько увидит в платежном поручении получатель, если плательщик закодирует 10 рублей в двоичном виде, а получателю это число придет без изменения. Сколько составляют издержки банка при осуществлении такой сделки, когда будет обнаружен дефект на стороне банка?



**Ответ:** Вы наверняка верно рассчитали 1010 рублей будет перечислено получателю, а банку будет нанесен ущерб 1000 рублей.

Итак, если с синтаксической адекватностью понятно что она определяет лишь равнозначность формального представления, то давайте рассмотрим семантическую адекватность. Семантической адекватность информации определяет смысловую степень соответствия образа объекта самому объекту.

Например, про те же платёжные поручения, но одна сторона выполняет платёж в долларах, а другая сторона производит зачисления той же суммы в рублях. Исходя из текущего курса, в отличие от предыдущего примера, Банк получит крупную сумму в результате такой операции, ведь он получит прибыль равную курсовой разнице. Но разумеется, репутационные риски сведут все прибыли банка на нет, и он будет вынужден компенсировать все издержки.

Подобный случай отсутствия адекватности информации будет наблюдаться, если мы рассмотрим пример платежного поручения с перечислением по номеру счёта, в котором будет указан номер карты получателя. В данном случае, если система не готова принимать номер карты вместо номера счёта, информация о номере карты будет воспринята системой как потребительски неадекватная, или по-другому у этой информации будет недоставать прагматической адекватности.

Прагматическая адекватность является третьим типом адекватности информации, и отражает соответствие информации цели её использования потребителем.

Следующим важным качеством информации является актуальность.

**Актуальность** информации напрямую связана с прагматической адекватностью, то есть с сохранением ценности информации для потребителя в момент применения. Приведите пример актуальной и неактуальной информации. Вспомните, с чем вы столкнулись, когда получили неактуальную информацию, призывающие вас к действию.



**Ответ:** Скорее всего Вы вспомнили неактуальный прогноз погоды, курс валюты и расписание занятий или транспорта.

Мы же, рассматривая один сквозной пример постараемся синтезировать о случае неактуальности сведений, для того чтобы показать важность этой характеристики информации.



Допустим, в платёжном поручении указана фамилия Петрова Елена Петровна, но ко времени проведение операции, она вышла замуж, сменила фамилию и подала документы в банк, что она является Ивановой Еленой Петровной. Разумеется порядочная финансовая организация хранит полную историю подобных изменений, но в случае если данный платёж первый, а счёт был открыт сразу по новой фамилии, возможен отказ зачисление средств по причине неактуальности сведений.

Тот же эффект будет если получатель средств закроет счёт, но откроет другой. В этом случае платёж точно невозможно будет зачислить. Все это ярко иллюстрирует важность этой характеристики информации.

Информация не может храниться вечно, у любых сведений должен быть определен жизненный цикл от появления до уничтожения. Отсутствия внимания к жизненному циклу информации ведет появлению проблем с её хранением, которое всегда не бесплатно.

Следующий из важных показателей качества информации это её доступность. Доступность информации – это такая характеристика, которая показывает возможность воспринимать информацию со стороны потребителя. Если бы мы говорили про человеческое восприятие, и я бы использовал не знакомый вам язык или диалект, то эта информация не была бы доступна вам без перевода.



С другой стороны, есть множество людей которым недоступна визуальной информация, но для помощи им был разработан специальный алфавит азбука Брайля, представляющий собой рельефно-точечный тактильный шрифт. Тексты Брайля, полученные тиснением бумаги позволяют незрячим людям читать, то есть устраняют проблему доступности информации.

Информационные системы в их современном представлении являются намного более примитивными чем человек, что для человека является естественным, то для информационной системы требует отдельного алгоритмического описания подчас весьма и весьма сложного.

Поэтому компьютерную информационную систему можно воспринимать в качестве строго ограниченной По формату приема и передачи информационных ресурсов. Поэтому доступность информации влияет любое отклонение от согласованного формата представления обмена данными. Например, при изменении правил кодирования или ключей шифрования информация становится недоступной для восприятия информационной системы. Такая информация утрачивает, иногда безвозвратно, важнейшее качество доступности, что делает её не применимой для целей управления и ненужной.

Говоря о языковых группах и нациях, необходимо помнить о существовании большого числа особенностей написания чисел и дат у разных народов, говорящих на одном языке. Например, американцы и англичане используют разные системы измерений (дюймовая и метрическая), а так же системы учета температур и дат.

Следующая характеристика информации является её достоверность.

**Достоверность** информации, это самая опасная характеристика. Ей уделяет повышенное внимание целый раздел информационных технологий под названием обеспечение информационной безопасности. Давайте разберёмся в чем же дело, и в чем же уникальность этой характеристики.

Представьте что в нашем сквозном примере допущена ошибка в одном из реквизитов платёжного поручения. Как это получилось, и к чему это приведёт? Какие у вас версии?

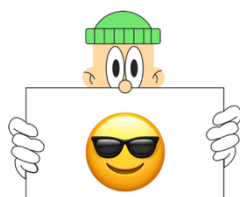
## К чему может привести ошибка в одном из реквизитов платёжного поручения?

**Ответ:** Самая банальная ошибка это техническая, связанное с вводом информации. Такая ошибка может привести к отказу от зачисления, неверной сумме перечисления, и в редчайших случаях к неверному адресату зачисления. Да предоставленную информацию нельзя назвать достоверной. Но это лишь один пример.

Другой пример касается преднамеренного искажения информации. Когда на стороне клиента или на стороне банка, одно из лиц или автоматизированный процесс вносят случайно (или преднамеренно) такие изменения в информацию, что она перестаёт соотноситься с первоначальной.

Примером таких искажений может быть техническое разделение платежей на несколько отдельных транзакций. И так как сумма каждой транзакции не соответствует изначальной, то они не будут сходиться с оригинальной информацией, то есть при разделении потеряется признак достоверности, лишь отдельным алгоритмом он может быть восстановлен.

Другой случай произойдет, когда информация искажена, и в случае если это было сделано умышленно, платёж будет осуществлен по подложным реквизитам. То есть, переданное в платёжном поручение недостоверной информации приведёт к зачислению денежных средств по подложным реквизитам или другой сумме.



Это настолько опасная характеристика информации, что в банковской среде и специальные автоматизированные системы отслеживают направление платежа и сумму для исключения воспроизведения подобных сценариев.

В других же сферах деятельности существуют разные правила работы с недостоверной информацией. И например, различные прогнозы имеют низкую степень требований достоверности, а информация таможенного декларирования товаров при пересечении границы, имеют настолько высокие требования к достоверности, что любое нарушение таможенных дисциплины трактуется как умышленное правонарушение.

Современные технологии глубокого обучения нейронных сетей позволяют в режиме реального времени подменять лицо или голос удаленного собеседника. Такие технологии используются уже не только для розыгрыша, но и для воздействия на полномочного сотрудника в корыстных целях. Известен случай когда подобные ролики запускали мошенники для создания видимости авторитетного бизнеса.

Говоря о качестве информации ещё рассматриваются такие характеристика как:

- содержательность – это отношение семантически важной информации к её общему объему;
- репрезентативность, показывающая корректность выборки анализируемой информации из общего потока;
- точность, раскрывающая степень близости информации к реальному объекту.

Устойчивость, отражающая способность реагировать на изменение исходных данных без критической потери точности.

Но описанные четыре характеристики информации массово применяются при аналоговом представлении информации и непрерывном взаимодействии. Но в цифровых информационных системах с дискретным принципом взаимодействия либо неприменимы, либо отходят на второй план и реализуются в основном за счет использования соответствующих стандартных низкоуровневых протоколов обмена, обеспечивающие эти качества.

Но ситуация меняется при проектировании нагруженных систем, где на больших объемах передаваемой информации взаимодействия становятся непрерывными и данные показатели информации напрямую влияют на надежность системы.

# Особенности использования бизнес информации

Важно и то, что информация в экономических системах должна быть защищена, так как представляет значительную ценность для целей управления и текущей деятельности. Её искажение, подмена и разглашение сведений о хозяйствующем субъекте или лицах с ним взаимодействующими может нанести значительный материальный ущерб.

Предприятиям и организациям предписано соблюдать режим коммерческой тайны, а банковскому сообществу – банковской тайны. Так, сведения о поставщиках и подрядчиках относятся к коммерческой тайне, реквизиты платежных документов составляют банковскую тайну, но и персональные данные физических лиц – граждан РФ также подлежат строгой защите.

Давайте разберемся с основными нормативными актами, которые регулируют обращение и обработку данных.

Ниже рассмотрим основные нормативные акты.

**№-63 ФЗ «Об электронной подписи»** — закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Закон вводит понятие **электронной подписи** — информация в электронной форме, которая присоединена (отнесена) к другой информации в электронной форме — подписываемой информации, и однозначно гарантирует её целостность.

Выделяют прикрепленную, то есть содержащуюся внутри документа электронную подпись и открепленную, которая хранится в отдельном файле.

Электронная подпись представляет собой совокупность сведений о подписанте, времени и месте подписи, а также содержит хэш-функцию самой подписи, которая может быть проверена с использованием алгоритмов открытого ключа, без возможности внесения в неё изменений. Кроме как с использованием закрытого ключа, который известен только подписанту.



Почему электронная подпись настолько важна? С одной стороны, мы привыкли иметь дело с электронными сообщениями вместо бумажных документов, но как гарантировать, что электронное сообщение выражает изначально вкладываемый в неё смысл? Как гарантировать неизменность сообщения, так чтобы оно не потеряло юридической значимости?

Допустим клиент банка, работая в интернет банке, ошибочно формирует распоряжение на перечисление денежных средств с неверными реквизитами. Два нажатия в личном кабинете и платеж отправляется на провод по балансу, проводится, и с этого момента считается безотзывным. Спohватившись клиент сообщает банку, что произошел технический сбой, в результате которого с его счета списались денежные средства.

Возникает конфликтная ситуация. Разрешить её помогает электронная подпись. Если автоматизированная система банка спроектирована грамотно, то помимо сообщения для его исполнения требуется его заверение подписью клиента. Конечно, клиент может быть приглашен в отделение банка для собственноручного подписания платежной инструкции, но скорее всего после первого похода в банк клиент сменит обслуживающую финансовую организацию — попросту перейдет в другой банк на обслуживание.

Итого, давайте разберемся какие возможности у клиента есть в части электронного подписания? Первое, что приходит на ум — это ввод кода подтверждения, полученного через СМС уведомление. Так называемый пин-код является средством создания простой электронной подписи (ПЭП). Но не все так просто, данная подпись может быть приравнена к собственноручной, если она завязана на персональные данные подписанта, например СНИЛС, что дает возможность однозначно соотнести электронную подпись не только с приписываемыми данными, но и с владельцем электронной подписи.

Федеральный закон №152, который мы будем разбирать ниже предъявляет требования по предварительному получению согласия на обработку персональных данных, прежде чем с их помощью будет сформирована хэш-функция электронной подписи.

Второй тип подписи это усиленная электронная подпись, делящаяся на два вида, усиленная квалифицированная электронная подпись (УКЭП) и усиленная неквалифицированная электронная подпись (УНЭП).

**Неквалифицированная усиленная электронная подпись** согласно ФЗ обладают уже гораздо большим спектром возможностей. Эта электронная подпись создаётся программами криптошифрования с использованием закрытого ключа. С её применением идентифицируется личность обладателя и обнаруживается факт внесения в файл изменений.

Клиент получает в УЦ два ключа ЭП: закрытый и открытый. Первый хранится на ключевом носителе с ПИН-кодом или в ПК владельца и известен только ему. С ним пользователь создаёт ЭП для её дальнейшего проставления. Открытый, доступен всем сторонам электронного документооборота. Он связан с закрытым и позволяет получателям документа узнать, подлинна ли подпись.



В момент подписания пользователю должны быть доступны для просмотра содержание подписываемого электронного документа, которое обычно отображается в интерфейсе подписания

Эту ЭП можно использовать в любом виде электронного документооборота, но во внешнем, стороны заключают соглашение о правилах использования и обоюдном признании юридической силы.


Усиленная квалифицированная электронная подпись. Как и предыдущий вид, эта подпись создаётся при помощи криптографии и открытых ключей. Но по правилам 63 ФЗ отличается квалифицированная подпись тем, что она имеет квалифицированный сертификат. ПО для работы с ней должно быть сертифицировано ФСБ. Также согласно 63 ФЗ квалифицированная электронная подпись выдаётся только УЦ, аккредитованным Минкомсвязи.

Исходя из 63 ФЗ, квалифицированная электронная подпись усиленная не требует дополнительных условий и соглашений от участников обмена. Такая подпись по закону применима для:


- отчётности в госорганы;
- электронных торгов;
- работы с ИС любого органа государственной власти;
- внутрикорпоративного и внешнего электронного документооборота.

Существенная разница УКЭП и УНЭП заключается в порядке отзыва сертификата. Сертификат подлежит отзыву в случае раскрытия закрытого ключа или при прекращении отношений между юридическим лицом и его представителем, на которое был оформлен сертификат электронной подписи.

Дело в том, что электронная подпись сформированная на отозванном сертификате не имеет юридической силы, а значит при проверке действительности электронной подписи следует проверять действие сертификата ключа, на котором ЭП была сформирована. Если УНЭП контролируется по соглашению между участниками обмена электронными документами, то УКЭП контролируется через взаимосвязанную систему удостоверяющих центров и при правильной организации работы с ЭП позволяет обнаружить факт отзыва электронной подписи сразу после наступления такого события.


 Применяйте усиленную квалифицированную электронную подпись (УКЭП) для особо важных документов, а в случае недоступности федеральной системы удостоверяющих центров применяйте УНЭП. В случае клиентского обмена применяйте ПЭП для удобства обмена с клиентом

В рассмотренном примере банку будет просто доказать, что клиент действовал самостоятельно формируя ошибочную операцию и об этом будет свидетельствовать электронная подпись под документом (сообщением), однозначно свидетельствующая о целостности документа и идентифицирующая лицо, подписавшее документ.

 При использовании ПЭП и УНЭП подписания обязательно заключайте соглашения об использовании и признании электронной подписи

ФЗ №-152 О персональных данных — сведения позволяющие однозначно определить физическое лицо относятся к персональным данным и подлежат защите.

Идентификация подписанта является одним из важных, но не единственным применением персональных данных. Как говорилось ранее персональные данные позволяют однозначно определить физическое лицо участвующее в бизнес процессе.

 Хотя ФИО является персональными данными, но на основании только этих сведений идентифицировать человека бывает сложно. Помимо однофамильцев встречаются и полные тезки, поэтому только ФИО без привязки к другой информации суды не считают персональными данными.

Итак, **персональные данные** – это прямо или косвенно относящаяся к физическому лицу информация, с помощью которой он может быть идентифицирован. К персональным данным относятся ФИО, паспортные данные, ИНН, СНИЛС, дата рождения, адрес (регион, город, улица, дом, квартира), образование, место работы, семейное и социальное положение, сведения о здоровье, уровень дохода и т.д., то есть, любые сведения, по которым можно идентифицировать человека.

Любые действия с персональными данными, в том числе сбор, хранение, обработку и передачу организация осуществляет только после получения согласия на обработку персональных данных, и только в соответствии с целями использования перечисленными в согласии.



Стоит учитывать, что согласие на обработку персональных данных может быть отозвано субъектом персональных данных

Другой закон ФЗ №395-1 «О банках и банковской деятельности» Ст. 26 регулирует сведения, относящиеся к банковской тайне относится информация о банковских операциях, счетах и вкладах клиентов.

Следующий закон ФЗ №231 «О коммерческой тайне» ограничивает оборот сведений составляющих коммерческую тайну.

На практике выделяют следующие виды коммерческой тайны:

- информация о материальном положении фирмы;
- сведения о разработках компании (ноу-хау, промышленные образцы);
- данные о клиентах, контрагентах и прочих партнерах организации;
- информация об имуществе предприятия и его стоимости;
- прочие сведения коммерческого характера.

Это может быть, например, рецепт фирменного напитка, алгоритм или специально разработанная технология, информация о будущих скидках, планы развития или активная клиентская база. Каждая организация имеет право хранить такие данные в закрытом доступе, если правильно оформит документы устанавливающие режим коммерческой тайны на предприятии.

Коммерческая тайна обладает высокой ценностью именно потому, что закрыта от посторонних.

Наряду с банковской и коммерческой тайной выделяют государственную тайну и совершенно секретные сведения, доступ к которым строго ограничен и

регулируются отдельными нормативными документами специализированных регулирующих органов.

За разглашение, искажение, подмену или злоупотребление защищаемой информацией следует персональная уголовная ответственность.

Принципы обработки бизнес информации включают в себя сохранность, неизменность, конфиденциальность, персональную ответственность и принятие рисков.



#### **Сохранность и неизменность**

Системы должны обеспечивать хранение и неизменность ретроспективных данных. Сроки хранения устанавливаются по ведомственным нормативам. Так для банковской информации установлен срок 5 лет.



#### **Персональная ответственность**

Любая информация, обрабатываемая в бизнес системах должна содержать идентификацию источника информации, а в случае получения информации от физического лица – его реквизиты.



#### **Финансовые риски**

Бизнес информации свойственны финансовые и операционные риски. Снижение качества информации в конечном счете приводит к потерям.



В бизнес системах накладываются повышенные требования по качеству информации, этот факт следует учитывать при их проектировании

Поэтому в качестве основной требуемой процедуры выступает формально-логический контроль, в обязательном порядке предваряющий любой этап обработки информации, а также аутентификация источника и получателя информации, с обязательным протоколированием результатов обработки.

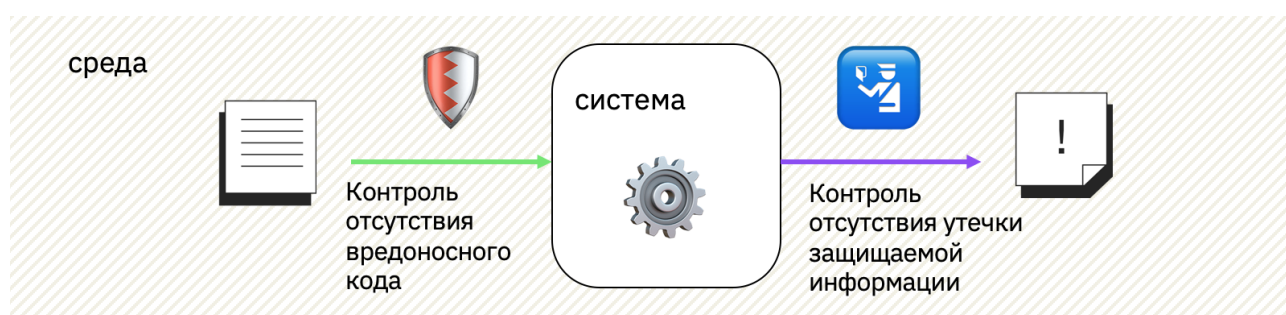
Дополнительно, на входе в информационную систему, информация должна в обязательном порядке проходить контроль на отсутствие вредоносного кода – программных средств, способных активизироваться на стороне получателя и нарушить логику работы системы, заблокировать её или привести к утечке информации.



Один из основных каналов поступления вредоносного кода — это электронная почта, взаимодействие с которой, должно быть ограничено. Должны быть созданы условия при которых очевидно с какой

Информацией внешней или внутренней имеет дело потребитель (сотрудник компании или алгоритм).

На выходе из системы в среду, должен осуществляться контроль на отсутствие защищаемой информации, не предназначенной для передачи в среду. Для исключения передачи сведений включая персональные данные или реквизиты платежных инструментов информация эта информация принудительно искажается, для того чтобы ей не могли воспользоваться злоумышленники, но у потребителя информации оставалось однозначное понимание о её контексте. Так номера банковских карт за исключением последних 4 цифр маскируются, что означает замену остальных символов на «\*» (символ звёздочки).



💡 Номера банковских карт — это защищаемая информация, утечка которой способна привести к совершению мошеннических действий с клиентскими средствами, поэтому такая информация должна выгружаться во внешнюю среду только в маскированном виде.

Оценка качества информации служит целям определения требований к системе, что является принципиальным прикладным вопросом проектирования и будет рассмотрено в следующей лекции.

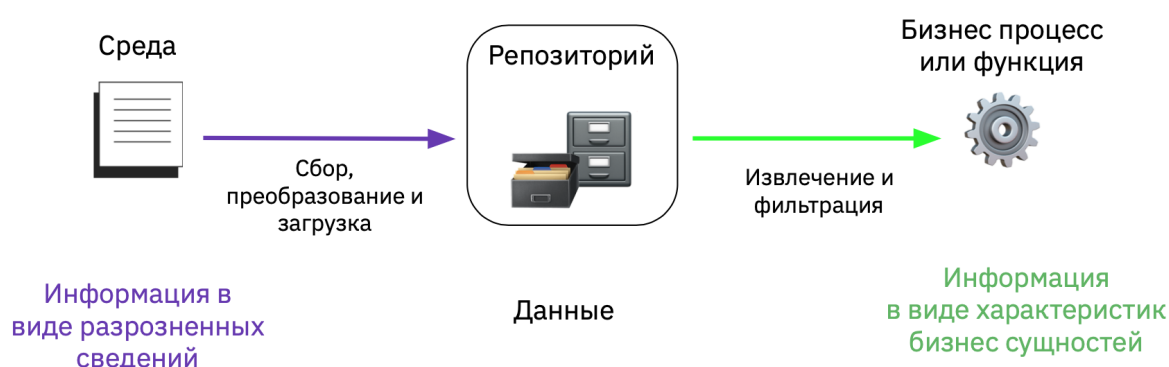
Говоря об информации, мы имеем в виду передаваемые и обрабатываемые сведения. В случае сохранения информации на носитель мы говорим уже не об информации, а о данных.

## Управление данными

Говоря об информации мы предполагаем, что доступная информация извлечена, преобразована и доступна для обработки. Значительные объемы обрабатываемой информации породили проблему сохранения и последующего использования

данных. Прежде всего стоит отметить, что вся информация не может быть одновременно доступна для обработки. С другой стороны огромный объем потенциальной информации представлен в виде данных, которые требуют проведение предварительных процедур для преобразования к виду, пригодному для машинной обработки.

Современные системы оперируют понятием “Озеро данных”. Озеро данных — это централизованный репозиторий, используемый для приема и хранения больших объемов данных в их исходном виде. Затем эти данные могут быть обработаны и использованы в качестве основы для различных аналитических задач и бизнес процессов.



Указанная проблематика относится к сфере управления качеством данных или Data Governance.

Data Governance – это совокупность процессов определения наиболее важных данных для использования, управления жизненным циклом и атрибутами качества, присвоение им прав доступа и управления для работы бизнес-процесса, а также защита данных от внешних воздействий.



Чем лучше организация управляет данными, тем дешевле обработка и хранение этих данных

Стоит отметить, что многие путают понятия Data Governance и Data Management. Data Management это процесс сбора, хранения и обновления данных.

Можно сказать, что Data Governance формирует стратегию управления данными и их жизненным циклом, а Data Management напрямую осуществляет управление данными согласно определенной стратегии.

Основными характеристиками Data Governance являются:

- Доступность;
- Удобство;
- Целостность;
- Стоимость;
- Безопасность.

Таким образом, управление качеством данных имеет целью повышение доступности, надежности и показателей качества данных с одновременным выявлением и снижением потенциальных рисков обработки данных, в том числе за счет поддержания соответствия реализуемого процесса работы с данными и законодательной базы, которую мы обсудили ранее.

Основой для ведения деятельности по руководству данными выступает бизнес глоссарий.

Бизнес-глоссарий устанавливает общее понимание терминов в организации, определяет бизнес-термины для понимания человеком. Это единая лексика внутри организации, которая оформляется в виде алфавитного списка терминов и их определений, может содержать: аббревиатуры, синонимы, описания бизнес-правил.

Существует множество международных бизнес глоссариев, так в банковской сфере широко распространен глоссарий BIAN.

Banking Industry Architecture Network – это ассоциация архитекторов банков, поставщиков банковского программного обеспечения и провайдеров услуг с общей целью создания стандартной семантической среды банковских сервисов.

В стандарте BIAN для проектирования бизнес-архитектуры используется подход выделения областей бизнеса (сервисных доменов) и связанных услуг (сервис-операций), которые могут быть выделены и объединены в модели любого банка (или финансового предприятия).

Модель BIAN является «канонической», что означает, что её можно использовать любым банком независимо от её последующих технических реализаций. Для определения «канонической модели BIAN» подход к её проектированию должен принципиально отличаться от более традиционных процессно-ориентированных методов. BIAN использует подход сервис-ориентированной архитектуры (SOA).



Управление качеством данных объединяет основные данные в рамках всей организации и обеспечивает централизованное управление, с этой целью формируется единое бизнес представление данных.

В качестве примера проблемы можно привести следующий кейс: в зависимости от процесса, атрибут “Счёт” может быть представлен разными сущностями, например для кредитования — это “Судный счёт”, а для депозитных операций физических лиц это “Накопительный счёт” или “Валютный счёт”, для предприятий это может быть “Расчётный”, “Дополнительный” или “Специальный” счёт. А может быть совершенно другой сущностью, например “счёт на оплату”.

При использовании понятий в сквозных процессах может происходить мутация данных. Так например, отчет по просроченной задолженности может охватывать не только ссудные, но и расчётные счета. Соответственно, данные полученные с использованием такого отчета будут содержать ошибку, которая может проявляться не всегда, а лишь в зависимости от исполненных операций, что многократно затрудняет отладку и тестирование.

Но даже такая с виду незначительная единичная ошибка, может привести к значительным потерям организации, если речь идет о выполнении значительных, массовых или критически важных операций. И уж точно подобная ошибка приведет к общему снижению доверия к данным, что породит каскадный эффект по доработке систем для обеспечения дополнительного контроля данных.

Такой контроль данных с точки зрения управления качеством данных является избыточным, а само управление качеством данных позволяет существенно оптимизировать процессы формато-логического контроля.



Управление качеством данных направлено прежде всего на повышение доверия к данным, что существенно снижает издержки связанные с многократной повторной фильтрацией, преобразованием и анализом данных

К основным функциям реализуемым руководством данными относятся руководства данными:

- ведение концептуальной и логической модели данных;
- каталогизацию метаданных, выделение сущностей и атрибутов;
- создание и ведение дополнительных категорий метаданных, списков и ролей заинтересованных лиц;

- управление жизненным циклом данных;
- настройка процессов согласования (например, бизнес-терминов);
- построение связей между логической и физической моделями данных;
- отслеживание и визуализация текущих показателей качества данных.
- 

Между тем есть несколько понятных принципов, на которых базируется стратегия управления качеством данных.

### 💡 Обеспечьте доступность ваших данных

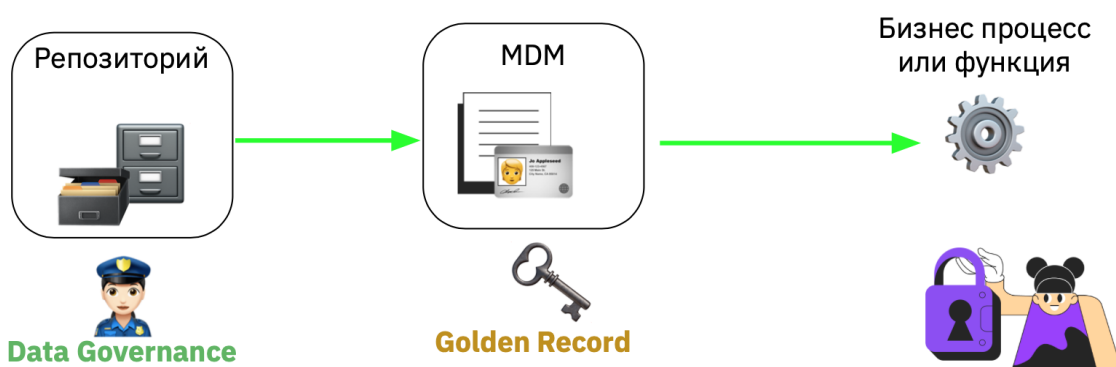
Ни одна «умная» система не будет работать в полную силу, если у нее нет доступа к необходимой информации. Но здесь нельзя забывать о конфиденциальности: уже при составлении стратегии качества данных важно понять, какие данные и в каком виде должны быть доступны клиентам и специалистам компании.

Например, если речь идет о банке, то номер банковской карты должен быть частично скрыт от пользователей, кроме тех кто осуществляет непосредственный ввод этих данных.

### 💡 Пользователи и процессы должны работать с согласованными данными

Ситуация, когда сотрудники разных подразделений работают с разными экземплярами данных, может привести к тому, что в результате решения схожих процессах будут совершенно разными.

Современный подход, решающий эту проблему заключается в построении централизованных DWH/DataLake. В такой однозначно обозначены системы отвечающие за мастер данные и процедуры согласования данных.



Система в которой содержатся наиболее достоверное, проверенное, непротиворечивое и полное представление об объекте, его эталонное состояние — называется мастер данными (MDM - англ. master data management). А сами эталонные записи называются “золотой записью” (англ. Golden Record).

Например, процедура дедупликации клиентских карточек является головной болью сложных клиентоориентированных информационных систем, так как клиент может быть зарегистрирован в разных системах в разном качестве. Например, бухгалтер одновременно может быть клиентом, физическим лицом, работником одной организации, в которой он получает заработную плату. И представителем другой организации, в которой он осуществляет функции бухгалтера.



Необходимо ясно понимать, что собирать и хранить, а что игнорировать и удалять

Не собирайте бесполезный «мусор»: использование нерелевантных или безнадежно устаревших данных для принятия управленческих решений вряд ли позволит повысить конкурентоспособность компании.

Стратегия управления данными предполагает, что место в хранилище должны получать только актуальные сведения.

Конечно, навсегда удалять данные, не соответствующие критериям качества необязательно. Но продуманная архивная политика удовлетворяющая требованиям по времени обязательного хранения данных необходима как в компании в целом, так и в каждой отдельной системе.



Обеспечьте сохранность данных

Обеспечение надежности и резервного копирования, является неотъемлемым условием обеспечения качества данных. В значимых системах рассматриваются вопросы устойчивости, предполагающие подготовку ответа на вопрос функционирования системы в условиях чрезвычайной ситуации и потери части организационной инфраструктуры.



Позаботьтесь о безопасности данных

В общем все вопросы исполнения требований законодательства относительно обрабатываемой информации и хранимых данных относятся к комплаенс, без решения которых не обходится ни один бизнес процесс.

В общем, стратегию работы с данными можно сравнить с управлением финансами: последние необходимо держать в порядке и поддерживать с помощью аудита и различных инструментов контроля. Не менее важно обеспечить сохранность денежных средств. По факту данные – это такой же актив, а в современном мире иногда даже более ценный, поэтому к нему применимы все те же правила: как и грамотное управление финансами, Data Governance помогает уменьшить количество ошибок, повысить эффективность бизнеса и ясно понимать – каких результатов можно достичь в дальнейшем.

Таким образом, управление качеством данных или Data Governance выступает связующим звеном между бизнесом и системной архитектурой, позволяя поддерживать качество данных на всем протяжении их жизненного цикла и в любых процессах, что приводит к существенному росту их качества и экономии, как в процессе развития, так и в процессе эксплуатации.

## Заключение

Итак, мы рассмотрели основные характеристики качества информации рассматриваемые при проектировании информационных систем. Эти характеристики включают полноту, адекватность, актуальность, доступность, достоверность, содержательность, репрезентативность, точность и устойчивость информации.

За вопросами низкого качества информации в бизнес системах стоят финансовые риски и потери со стороны заказчиков и потребителей проектируемых информационных систем.



Полнота, адекватность, актуальность, доступность и достоверность – основные показатели качества информации

Построение современных систем обрабатывающих бизнес информацию в настоящее время немыслимо не только без оценки качества всей используемой

информации, но и без разработки процедур поддержания и обеспечения надлежащего качества информации.

## Что можно почитать еще?

1. Для лучшего изучения темы можно почитать [Курирование данных и качество данных](#)
2. РОУНБ им. Горького, методическое пособие [«Критическая оценка информации»](#)
3. Инфраструктура простой электронной подписи. [«Практические аспекты реализации»](#)
4. [«Референтная модель BIAN»](#) для банковской индустрии или как перестать изобретать велосипед

## Используемая литература

1. В. В. Лидовский «Теория информации»
2. Симонович С.В. «Информатика. Базовый курс: Учебник для вузов»
3. Казанский (Приволжский) федеральный университет «Учебно-методический комплекс Методы анализа и сбора бизнес-информации»
4. Е. О. Фроленкова, Информационно-прикладные системы оптимизации и управления бизнесом
5. Н. В. Костылева, Ю. А. Мальцева, Д. В. Шкурин, Информационное обеспечение управленческой деятельности : учебное пособие