**Лекция 1. Управление транзакциями**

**1. Теоретические модели**

Транзакцией называется конечный набор операций над базой данных, который переводит одно согласованное состояние базы данных в другое при условии, что все операции выполнены полностью и без помех со стороны других транзакций.

Неформально требования к транзакционным системам характеризуются свойствами ACID (атомарность, согласованность, изоляция и долговечность).

Средства управления транзакциями решают *задачи*:

• поддержка базы данных в согласованном состоянии при нормальной работе системы;

• восстановление согласованного состояния при отказах (транзакций, системы или носителя данных)

**1.1. Критерии корректности конкурентного  
выполнения**

Формальные модели корректности

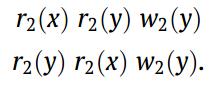
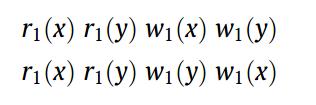
Классическая теория транзакций использует очень простую модель:

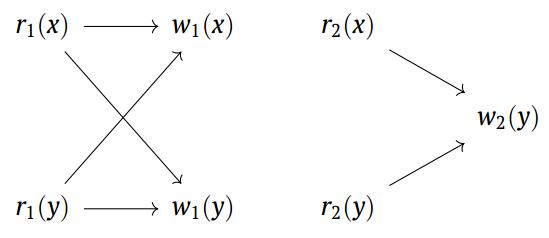
- считается, что база данных состоит из независимых и никак между собой не связанных элементов данных, которые обозначаются x,y,... Над этими элементами можно выполнять операции чтения r и записи w, при этом каждая операция выполняется в рамках какой-либо транзакции. Так, операция r1(x) относится к транзакции 1 и читает x, а операция *wi(y)* записывает y в транзакции i.

Над множеством операций (из транзакций) введем бинарное отношение частичного порядка - предшествование.

Операции над каждым элементом данных упорядочены полностью.

Бинарное отношение (два атрибута). Отношение эквивалентности (рефлексивное, симметричное, транзитивное). Отношение частичного порядка (антисимметрично, транзитивно) или упорядоченность. Полная упорядоченность (линейный порядок).





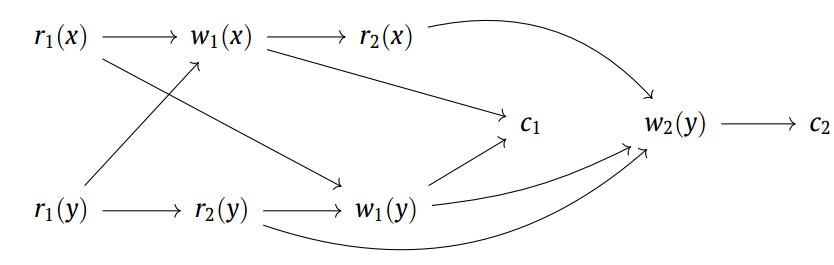
**1. 1. 1 Формальные модели корректности**

**Историей** для конечного набора транзакций называется множество всех операций этих транзакций,

* снабженное отношением частичного порядка, согласованным с отношением порядка операций внутри транзакций и таким, что
* все операции над одним элементом данных полностью упорядочены.

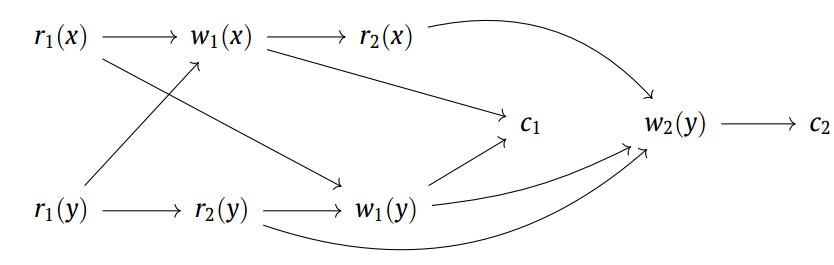
История может быть представлена

* в частично упорядоченном виде;
* в полностью упорядоченном виде.

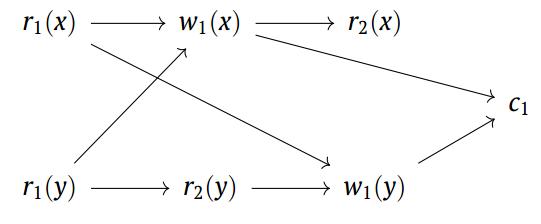


**Префиксом** частично упорядоченного множества называется подмножество, которое вместе с каждым элементом содержит все элементы, предшествующие ему в смысле частичного порядка.

**Расписанием** называется префикс истории.







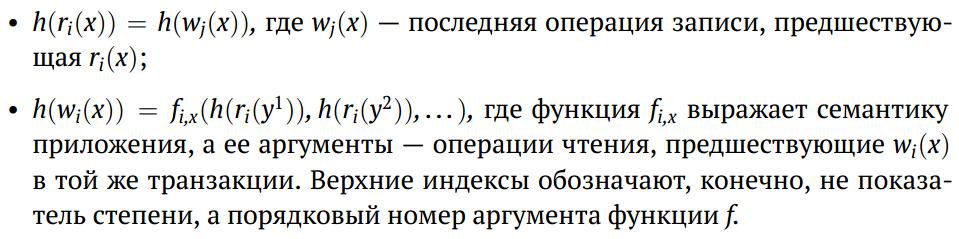
Расписание называется **серийным**, если для любой пары транзакций в этом расписании все операции одной транзакции предшествуют всем операциям другой.

Отношение предшествования для операций остается отношением частичного порядка, но транзакции в таком расписании полностью упорядочены.

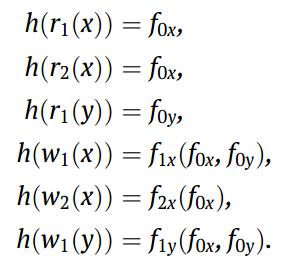
Далее предполагается, что каждая транзакция читает и записывает любой элемент данных **не более одного раза**, при этом если элемент записывается, то запись следует за чтением. Кроме этого, предполагается, что все операции оборванных транзакций уже исключены из расписания.

По определению транзакции, серийное расписание является **корректным**, т. к. каждая транзакция в нем выполняется полностью и без помех со стороны других транзакций.

**Семантика Эрбрана**

****

Используя функцию *h*, можно записать выражения, определяющие считываемые или записываемые значения для любой операции в расписании. Например, для расписания 



Истории называются **эквивалентными по конечному состоянию**, если построенные по ним семантики Эрбрана совпадают для t∞, и **эквивалентными по видимому состоянию**, если совпадают семантики Эрбрана для всех операций.

Расписание называется **сериализуемым по конечному состоянию** (FSR) или **сериализуемым по видимому состоянию** (VSR), если оно эквивалентно по конечному состоянию или видимому состоянию соответственно какому-нибудь серийному расписанию.

Проверка сериализуемости по видимому состоянию является NP-полной задачей.

Если можно доказать, что расписания из некоторого **класса** сериализуемы по видимому состоянию, то они будут семантически корректными.

Сериализуемость по конечному состоянию является слишком слабой (например, не предотвращает аномалию несогласованного чтения) и поэтому используется только теоретиками для сравнения с другими классами расписаний.

Очевидно, что VSR входит в FSR, т. е. любое расписание, сериализуемое по видимому состоянию, будет сериализуемо по конечному.

**Граф сериализуемости**

Конфликтом называется пара операций *pi*(x)🡪*qj*(x), такая, что:

1) Операции *p* и *q* применяются к одному и тому же элементу данных *x*;

2) Транзакции i и j различны;

3) по крайней мере одна из операций *p* и *q* является операцией записи *w*.

Расписания называются эквивалентными по конфликтам, если совпадают множества конфликтов, имеющихся в этих расписаниях.

Расписание называется сериализуемым по конфликтам (CSR), если оно эквивалентно по конфликтам некоторому серийному.

**Теорема**. CSR входит в VSR.

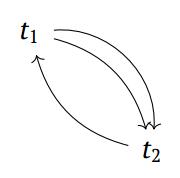
*Доказательство*. Пусть расписания S1 и S2

одного и того же множества транзакций неэквивалентны по видимому состоянию. Тогда найдется операция ri(x), такая, что в S1 последней предшествующей операцией записи будет wj(x), а в S2 — операция wk(x). В расписании S1 операция wk(x) будет либо предшествовать wj (x), либо следовать за ri(x). Аналогичные, но другие соотношения будут иметь место в S2. Следовательно операции будут располагаться в конфликтах в разном порядке, S1 и S2 не эквивалентны по конфликтами и CSR *⊂* VSR, т. е. эквивалентность по конфликтам обеспечивает семантическую корректность, ч.т.д.

**Графом сериализуемости** для расписания называется ориентированный мультиграф (граф, в котором любая пара вершин может быть соединена несколькими дугами), вершины которого соответствуют транзакциям, входящим в расписание, а дуги — конфликтам между операциями этих транзакций. Если для некоторой пары транзакций существует несколько конфликтов, то граф будет содержать несколько дуг, соединяющих соответствующие вершины.

**Критерий сериализуемости** расписаний по конфликтам.

Расписание **сериализуемо** по конфликтам ⬄ граф сериализуемости не содержит контуров (т. е. обладает свойством ацикличности).

**Коммутативность операций**

Понятие конфликта можно заменить на понятие коммутативности операций.

Две операции коммутируют, если выполняется хотя бы одно из следующих условий:

• операции не упорядочены в расписании (и, следовательно, могут выполняться в любом порядке);

• операции являются операциями чтения;

• операции выполняются над разными элементами данных разными транзакциями;

• операции выполняются над разными элементами данных в одной транзакции, но их порядок не определен в этой транзакции.

Сериализуемость по коммутативности эквивалентна сериализуемости по конфликтам.

Операции, находящиеся в конфликте, не коммутируют.

Если в результате применения таких трансформаций расписание может быть преобразовано в серийное, оно называется сериализуемым по коммутативности.

**Изоляция мгновенных снимков,   
snapshot isolation, SI**

Широко известные протоколы управления транзакциями на основе блокировок, гарантирующие все свойства корректных расписаний, слишком сильно ограничивают возможности конкурентного выполнения. Транзакции слишком часто оказываются в состоянии ожидания, в результате существенно ограничивается пропускная способность СУБД.

Необходимость глобальных блокировок делает эти протоколы немасштабируемыми и, следовательно, неприменимыми в распределенных системах.

В языке SQL предусмотрена возможность использования **ослабленных** критериев корректности (задаваемых уровнями изоляции), а реализации СУБД применяют протоколы, не гарантирующие корректность, но обеспечивающие более высокую пропускную способность.

Свяжем с каждой транзакцией:

1) метку времени начала транзакции STS(t);

2) метку времени фиксации транзакции CTS(t);

3) интервал времени, в течение которого выполнялась транзакция

τ(t) =(STS(t),CTS(t));

4) множество элементов данных, которые записываются транзакцией WS(t) (writeset).

При использовании протокола SI операции чтения возвращают значения, которые имели элементы данных на момент начала транзакции STS(t). Если транзакция модифицировала элемент данных, то она сама может прочитать новое значение, но другие транзакции смогут его получить только после фиксации транзакции, записавшей это значение.

Выполнение транзакций t1, t2 называется конкурентным, если

,

т. е. интервалы времени, в течение которого они выполнялись, имеют непустое пересечение.

Протокол SI допускает **конкурентное выполнение** транзакций, только если пересечение множеств записываемых ими элементов данных пусто (другими словами, не существует элемента данных, который записывается каждой из двух транзакций).

Формально это можно записать компактной формулой:



Режим Read Committed никогда не приводит к обрывам в PostgreSQL. Строго говоря, такие варианты нельзя считать реализациями SI.

Не рассматривается вопрос о том, какими средствами СУБД может гарантировать выполнение этого условия. Если условие нарушается, т.е. пересекаются как интервалы времени, в которые выполняются транзакции, так и множества записываемых значений, то одна из транзакций обрывается.

Правила SI гарантируют невозможность грязного чтения:

транзакция может читать результаты работы других транзакций только после их фиксации.

**Изоляция мгновенных снимков . Примеры**

1. Существуют сериализуемые по конфликтам расписания, которые не допускаются протоколом SI.

Например, в следующем расписании интервалы времени выполнения и записываемые множества непусты, но расписание сериализуемо по конфликтам.

2. В то же время протокол SI не гарантирует сериализуемость даже по конечному состоянию.

не сериализуемо по конечному состоянию, что доказывается вычислением семантик Эрбрана для этого расписания и для двух вариантов последовательного выполнения этих транзакций



допускается SI, т. к. записываются разные элементы данных

В приведенном расписании конечные значения x и y зависят только от начальных состояний, а при последовательном выполнении, например, t1 t2, значение x будет зависеть от значения, записанного первой транзакцией в y. Это расписание является примером аномалии несогласованной записи.

3. Можно доказать, что кроме аномалии несогласованной записи SI допускает аномалию только читающей транзакции. Для того чтобы исключить эти аномалии, вводится вариант сериализуемого протокола SI (serializable snapshot isolation, SSI).

Имеются конфликты между всеми парами транзакций, однако зависимость

есть только между первой и второй транзакциями.



Формальное описание этого протокола основано на понятии зависимости между транзакциями:

* зависимость WR возникает, если t1

записывает некоторый объект, который читает t2:



* зависимость WW возникает, если t1

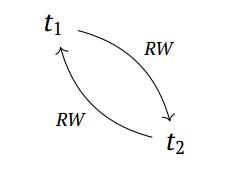
записывает некоторый объект, который t2 замещает:



* антизависимость RW возникает, если t1 записывает некоторый объект, а t2 читает предыдущее состояние этого объекта:



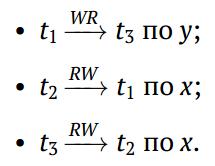
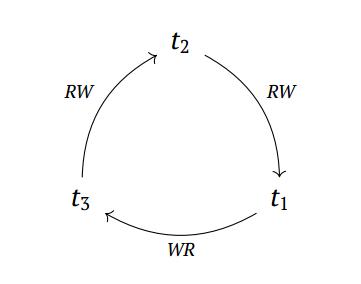
Аномалия несогласованной записи



Аномалия только читающей транзакции



Имеются следующие зависимости:

**Расписания с множественными версиями данных**

Одной из причин обрыва транзакции может быть попытка чтения данных, которые уже изменены другой, логически более поздней транзакцией.

Попытаемся выполнить ее, используя немного **устаревшие** значения необходимых ей элементов данных.

Использование **множественных версий** данных для управления транзакциями не связано с каким-либо конкретным методом управления транзакциями и может рассматриваться в сочетании с различными критериями корректности.

Каждая транзакция видит только **одну** согласованную версию базы данных.

Формализовать многоверсионность

Пересмотреть определения историй и расписаний

Пересмотреть определения критериев корректности

Версии одного элемента данных:

* записанных i-ой транзакцией
* читаемых j-ой транзакцией

, , 

Любая операция записи создает новую версию.

*Х*0 – начальное значение.

Пример:



1. Моноверсионное расписание.
2. Аномалия несогласованного чтения.



Корректное при многоверсионности

****

Аномалия потерянного обновления

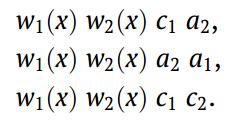
**Восстановимость**

Операция обращения записи - восстановление х до начала записи.

****

****

Некорректное расписание

****

Корректное расписание

Расписание называется восстановимым, если для любой пары операций



либо фиксация транзакции ti предшествует фиксации tj, либо tj обрывается. Класс восстановимых расписаний обозначается RC (recoverable).

Если при этом t1 обрывается, то перед ее обрывом выполняется обрыв t2 (несмотря на то что t2 была готова зафиксироваться).

Такой обрыв транзакции t2 называется **каскадным**.

Свойство **восстановимости** расписаний никак не соотносится с **сериализуемостью**:

восстановимое расписание может быть не сериализуемо даже по конечному состоянию, а сериализуемое по конфликтам расписание может не быть восстановимым.

Более сильное условие предотвращает аномалию грязного чтения: выполнение любой операции транзакции tj над элементом данных, записанным транзакцией ti, откладывается до завершения ti.

**Строгие расписания - ST.**

Чтобы предотвратить каскадные обрывы, необходимо отложить выполнение операции wj(x) до завершения транзакции ti. Расписания, удовлетворяющие

этому условию, называются **бескаскадными** **(ACA)**.

Задача 1. Доказать, что 

Задача 2. Доказать, что 

Задача 3. Доказать, что 

т. е. любое расписание из класса RG будет строгим и сериализуемым.

Расписания, в которых для любой операции транзакции ti любая конфликтующая операция транзакции tj над тем же элементом данных откладывается до завершения ti , называются точными (rigorous). **Точные расписания - RG.**

**Лекция 2. Управление транзакциями (продолжение)**

**1. Диспетчеры и протоколы**

Диспетчером транзакций будем называть программу (обычно входящую в состав ядра СУБД), которая отвечает за корректность выполнения транзакций. На вход диспетчера поступает упорядоченный (возможно, частично) поток запро сов на выполнение операций над базой данных, а на выходе должен получаться поток, выполнение которого удовлетворяет каким-либо критериям корректности. Диспетчер обеспечивает выполнение некоторого набора правил для каждой транзакции. Обычно подобные совокупности правил, обязательных для независимых взаимодействующих участников, называются протоколами (в отличие от алгоритмов, предписывающих определенные действия).

Протоколы управления транзакциями определяются так, чтобы гарантировать соблюдение требований к корректности расписаний при условии соблюдения правил протокола всеми транзакциями. Таким образом, диспетчер обеспечивает выполнение правил протокола каждой транзакцией, что в итоге приводит к соблюдению требований корректности расписания в целом.

Для того чтобы добиться корректности, диспетчер может:

• передавать поступившую операцию на выполнение немедленно;

• задерживать выполнение операции, пока не будут удовлетворены некоторые условия, например завершение другой транзакции;

• запрещать выполнение операций, что, в силу принципа атомарности, влечет за собой обрыв транзакции, которая запросила выполнение этой операции.

**Требования и критерии оценки**

Кроме **корректности**, диспетчер транзакций должен обеспечить **высокую производительность системы.**

Рассмотрим диспетчер, который запускает выполнение операций той транзакции, операции которой начали поступать раньше остальных, а операции всех других транзакций ставит в очередь.

После завершения транзакции такой диспетчер выбирает из очереди операцию, поступившую раньше других, и таким образом выбирает следующую транзакцию для выполнения. Этот диспетчер обеспечит получение на выходе серийного расписания, все критерии корректности будут выполнены, однако производительность системы будет крайне низкой из-за длительного ожидания в очереди.

**Основной метрикой**, определяющей качество диспетчера транзакций, является **пропускная способность системы**, определяемая как количество транзакций, которые система может выполнить за единицу времени.

**Пропускная способность зависит от:**

- возможностей оборудования;

- алгоритмов выполнения операций в СУБД;

- сложности этих операций;

- размеров транзакций.

Кроме перечисленных факторов, **пропускная способность зависит и от протокола, реализуемого диспетчером**. Диспетчер, по существу, блокирует возможность параллельного или псевдопараллельного выполнения транзакций, даже если оборудование и алгоритмы СУБД это позволяют.

Для практического измерения влияния свойств протоколов на пропускную способность используются **эталонные тесты (benchmarks)**, в которых все остальные параметры, влияющие на пропускную способность, зафиксированы.

Обычно эталонный тест предписывает определенную структуру и размеры базы данных, типы и размеры транзакций, поток которых поступает в систему при выполнении эталонного теста.

**Другой важной метрикой**, характеризующей качество протокола, является **доля транзакций, которые завершаются обрывом** из-за невозможности включить их в расписание, не нарушая правил протокола. Такие обрывы нежелательны, потому что:

* они снижают фактическую пропускную способность системы;
* на выполнение оборванных транзакций затрачиваются вычислительные ресурсы, а результаты выполнения при этом уничтожаются.

Доля обрывов зависит от многих параметров, поэтому и ее измеряют на эталонных тестах.

**Обе характеристики** протоколов (**пропускная способность** и **доля обрывов**) **зависят** от того, **как соотносятся по размеру активная часть базы данных** (то множество элементов данных, которые обрабатываются операциями транзакций) **и транзакции**: чем меньше база данных и чем длиннее транзакции, тем чаще одновременное выполнение таких транзакций оказывается невозможным.

В реальных базах данных активность всех элементов данных не может быть одинаковой, однако наличие элементов, которые очень часто обновляются очень многими транзакциями (такие элементы называются горячими точками, **hot spots**) может существенно ухудшить фактические значения характеристик системы.

Принято считать, что наличие таких горячих точек указывает на неудачное проектирование базы данных.

**Консервативные протоколы** предотвращают появление нежелательных (скажем, несериализуемых) расписаний. Такие протоколы тем или иным способом задерживают выполнение некоторых транзакций и тем самым снижают пропускную способность системы.

**Неконсервативные** протоколы позволяют увеличить степень параллелизма при выполнении транзакций, но могут увеличивать долю обрывов из-за невозможности удовлетворить требования протокола.

**Блокировки**

Большинство диспетчеров, реализованных в промышленных системах управления базами данных, для управления операциями транзакций использует блокировки (locks), называемые также замками.

Каждая блокировка связана с некоторым объектом базы данных (иногда с набором объектов) и с операцией, которая должна быть выполнена над этим объектом.

В простейшей модели базы данных **объектом является элемент данных**, а операцией — *чтение* или *запись*.

Если для некоторой операции используется **блокировка**, то она **устанавливается** **диспетчером до выполнения этой операции** (не обязательно непосредственно перед операцией) **и должна быть снята** после завершения операции и **не позже**, чем во время **завершения транзакции**.

**Все блокировки, установленные для транзакции, снимаются при ее завершении, если они не были сняты раньше.**

Некоторые протоколы могут обрывать транзакции при попытке установить несовместимую блокировку.

Блокировки могут быть совместимыми или несовместимыми друг с другом. Допускается одновременная установка совместимых блокировок разными транзакциями, а попытка установить блокировку, несовместимую с уже установленной, обычно приводит к тому, что транзакция переводится в состояние ожидания (ставится в очередь) и выводится из ожидания, когда все ранее установленные несовместимые блокировки снимаются.

Механизмы, близкие по назначению к блокировкам, используются не только в СУБД.

Подчеркнем важное отличие блокировок от таких примитивов синхронизации параллельных процессов, как семафоры и мьютексы (mutex): последние связаны с критическими участками программного кода, а не с объектами данных.

Для реализации механизма блокировок должны использоваться критические участки кода, защищаемые механизмами синхронизации операционной системы, но такая синхронизация необходима только на время выполнения операций установки и снятия блокировок, а не на все время, когда блокировка установлена.

Например, таблиц в базе данных значительно меньше, чем строк таблиц, поэтому таблицы обладают более крупной гранулярностью, чем строки, а значения отдельных атрибутов — более мелкой, чем строки.

Как **корректность**, так и **производительность** протоколов, использующих блокировки, **зависит** **от того, какие блокировки считаются совместимыми.**

Для того чтобы обеспечить, скажем, сериализуемость по конфликтам, необходимо (но не достаточно) сделать несовместимыми блокировки на операции, находящиеся в конфликте.

**Влияние диспетчера транзакций на пропускную способность системы зависит от того, насколько часто блокировки оказываются несовместимыми**, **и от гранулярности** (относительного размера) объектов, на которые блокировки устанавливаются.

Далее будем считать несовместимыми только блокировки, устанавливаемые для операций, находящихся в конфликте (не коммутирующих операций). В соответствии с определением конфликта блокировка для операции записи несовместима с любой другой блокировкой того же элемента данных.

В отличие от монопольных блокировок (на запись) блокировки на чтение не препятствуют установке других блокировок того же элемента данных на чтение, потому что операции чтения никогда не находятся в конфликте. Иногда **блокировки**, **допускающие установку некоторых видов блокировок того же элемента данных другими транзакциями, называются разделяемыми**.

В отличие от понятий «блокировка для чтения» и «блокировка на запись», термины «монопольная блокировка» и «разделяемая блокировка» не предполагают какую-либо семантику выполняемых операций, а определяют только свойства блокировок по отношению к другим блокировкам.

**2. Двухфазные протоколы, использующие блокировки**

Наиболее широко известным протоколом управления транзакциями, использующим блокировки, является двухфазный протокол блокирования (**two-phase locking, 2PL**).

В соответствии с этим протоколом для любой транзакции могут устанавливаться любые блокировки в любом порядке, однако после того, как хотя бы одна из установленных ранее блокировок снята, установка новых блокировок для этой транзакции запрещена.

Работа транзакции состоит из **двух фаз**: на первой фазе блокировки устанавливаются, на второй — только снимаются.

**Любые протоколы, основанные на блокировках, управляют только относительным порядком выполнения операций, с которыми связаны эти блокировки, но не зависят ни от типа блокировок** (монопольные или нет), **ни от типа объектов, ни от класса системы** (это совсем не обязательно должна быть СУБД).

Для того чтобы протокол был полезен для управления транзакциями, необходимо накладывать некоторые ограничения на используемые блокировки, различные для разных протоколов.

Для семейства двухфазных протоколов предполагается, что совместимость блокировок определяется наличием конфликтов между операциями, для которых устанавливаются блокировки.

Класс расписаний, которые могут быть получены в результате применения некоторого протокола управления транзакциями ***P***, обозначается ***Gen (P)***. Так, класс расписаний, порождаемый протоколом ***2PL***, обозначается ***Gen (2PL)****.*

**Теорема:** расписания, получаемые на выходе двухфазного протокола, являются сериализуемыми по конфликтам: ***Gen (2PL) ⊂ CSR***.

Для доказательства достаточно показать, что граф сериализуемости любого расписания ***s ∈ Gen(2PL)*** не содержит контуров. Пусть ***b(t)*** и ***e(t)*** обозначают соответственно операции установки последней блокировки и снятия первой блокировки для транзакции *t*. По определению двухфазного протокола ***b(t) < e(t)*** для любой транзакции ***t****.* Пусть **и**  обозначают операции установки и снятия блокировки на элемент данных ***x*** для транзакции и пусть в расписании имеется конфликт по элементу данных x между транзакциями и . Тогда



Следовательно, для любого пути , , ..., в графе сериализуемости имеет место

 и поэтому путь не может быть контуром, ч.т.д.

Протокол ***2PL***, как следует из доказанного утверждения, **гарантирует сериализуемость**, но **не обеспечивает восстановимость расписаний**. Действительно, **восстановимость зависит от порядка фиксации и обрывов, а не от упорядочения операций чтения и записи**, а завершение транзакций никак не регулируется блокировками.

Вариант, который называется **строгим двухфазным протоколом** *(****strict 2PL, S2PL***), отличается тем, что блокировки, установленные для операций записи, не снимаются до завершения транзакции.

Строгий двухфазный протокол генерирует расписания, которые сериализуемы по конфликтам и являются строгими: ***Gen(S2PL) ⊂ CSR ∩ ST***. Таким образом, на выходе ***S2PL*** получаются строгие, а следовательно, бескаскадные и восстановимые сериализуемые расписания.

Наконец, **точный двухфазный протокол *(rigorous 2PL, strong strict 2PL, SS2PL)*** требует, чтобы все блокировки удерживались до завершения транзакции. Класс расписаний, получаемых на выходе точного двухфазного протокола, совпадает с классом точных расписаний: ***Gen(SS2PL) = RG***.

Протокол ***SS2PL* полностью предотвращает** феномен грязного чтения, однако получающийся класс расписаний оказывается слишком узким и поэтому такой протокол не позволяет добиться высокой пропускной способности системы. По этой причине протокол ***SS2PL*** следует рассматривать как красивое теоретическое решение, очень редко (если вообще когда-либо) применяемое на практике.

Более точно, этот протокол был реализован во многих системах (до появления ***SI***), однако приложения, работающие с такими СУБД, использовали, как правило, ослабленные критерии согласованности, отказываясь от сериализуемости. Возможно, именно ограниченность этого протокола привела к включению ослабленных уровней изоляции в стандарт SQL.

**Тупики**

В системах, в которых используются блокировки (или другие средства синхронизации доступа к общим ресурсам, например семафоры), могут возникать ситуации тупика. Предположим, что для всех операций устанавливаются блокировки (как это требуется в двухфазных протоколах) и рассмотрим следующее расписание:



В этом расписании транзакция ожидает, когда транзакция снимет блокировку на элемент данных ***y***, при этом транзакция ожидает снятия блокировки на ***x***, которая никогда не будет снята, поскольку эта транзакция тоже находится в состоянии ожидания. Для возникновения тупика существенна несовместимость блокировок, а не тип выполняемых операций.

Точный алгоритм для обнаружения тупиков основан на понятии ***графа ожиданий***. Вершины этого графа представляют активные транзакции, а направленные дуги соединяют ожидающие транзакции с теми транзакциями, которые удерживают блокировки на ожидаемый элемент данных.

**Ситуация тупика имеет место тогда и только тогда, когда граф ожиданий содержит контур**. Этот алгоритм, однако, трудно реализуем в распределенных системах, поскольку информация о состояниях ожиданий может утратить актуальность за время, необходимое для сбора этой информации по сети, что может привести к обнаружению ложных тупиков.

После того как тупик обнаружен, его необходимо разрешить. Для этого достаточно оборвать одну из транзакций, оказавшихся на контуре. Существуют различные эвристические стратегии выбора жертвы: случайный выбор, с позднейшим временем начала и т. п.

Во многих СУБД в качестве альтернативы для поиска тупиков используется ограничение времени, в течение которого транзакция может находиться в состоянии ожидания.

Все упомянутые варианты двухфазного протокола блокирования несвободны от тупиков, однако существует несколько модификаций, в которых возникновение тупиков предотвращается, например:

• обрыв вместо ожидания — транзакция, которая пытается установить несовместимый замок, обрывается;

• обрыв по приоритету — все транзакции запускаются с низким приоритетом, при попытке установить несовместимую блокировку обрывается транзакция с меньшим приоритетом и ее приоритет увеличивается при повтором запуске;

• ожидание по приоритету — если несовместимый замок пытается установить транзакция с более высоким приоритетом, то низкоприоритетная обрывается, а если наоборот — то низкоприоритетная ожидает;

• по времени старта — ожидать может только транзакция, стартовавшая позже транзакции, удерживающей блокировку.

**Все варианты протоколов с предотвращением тупиков приводят к существенному увеличению доли оборванных транзакций**, поэтому их целесообразно использовать только в тех случаях, когда состояние ожидания нежелательно.

Например, вариант двухфазного протокола блокирования с обрывами вместо ожиданий применяется в системах транзакционной оперативной памяти.

**3. Другие протоколы на основе блокирования**

Не все протоколы, использующие блокировки, являются двухфазными. Протокол **WTL (write-only tree locking)**,предполагающий, что база данных структурирована в виде иерархического дерева. Работа этого протокола основана на том, что структура дерева накладывает ограничения на пути навигации в данных: допускаются только переходы от предков к потомкам. Этот протокол свободен от тупиков и мог бы применяться, например, для индексов. Однако для индексных структур известны более эффективные протоколы блокирования.

Простая модель базы данных, предусматривающая только операции чтения и записи, недостаточна для поддержки высокоуровневых языков запросов. Дело в том, что при ассоциативном доступе к данным (выборке данных по условию, например, как в операторах SQL, содержащих предложение WHERE) множество элементов данных (строк таблиц), обрабатываемых оператором, становится известно только во время выполнения оператора, что исключает возможность предварительной блокировки этих данных.

Решение (предложенное одновременно с двухфазным протоколом блокирования и дополняющее этот протокол) состоит в применении **предикатных блокировок**, **которые блокируют все записи, удовлетворяющие заданному условию**. Однако применение предикатных блокировок ограничивается тем, что задача проверки совместимости таких блокировок является в общем случае алгоритмически неразрешимой, а эффективные полиномиальные алгоритмы известны только для очень узкого класса предикатов (конъюнкций простых условий).

На практике применяются **мультигранулярные протоколы блокирования**, предусматривающие блокировки на объекты базы данных разного уровня (например, таблицы и строки таблиц) и накладывающие дополнительные ограничения на последовательность установки и снятия таких блокировок.

Применение блокировок на всю таблицу отрицательно влияет на возможность конкурентного выполнения транзакций, даже если такие блокировки устанавливаются лишь на короткий промежуток времени.

Отказ от использования предикатных (или мультигранулярных) блокировок может приводить к возникновению новых видов аномалий, которые появляются при повторном выполнении операций поиска, например:

• могут появиться новые строки, добавленные другими зафиксированными транзакциями и удовлетворяющие условиям поиска. Такие строки называются фантомами;

• строки, удовлетворяющие условиям поиска, могут быть изменены или удалены другой зафиксированной транзакцией и поэтому не будут найдены при повторном выполнении поиска. Такая аномалия называется неповторяемым чтением.

**Протокол на основе меток времени**

Критерии корректности расписаний не предполагают применение блокировок. **Протокол на основе меток времени (timestamp, TS)**, обеспечивающий сериализуемость расписаний с помощью альтернативной системы правил.

В рамках этого протокола каждая транзакция в начале своей работы (т. е. при регистрации транзакции в диспетчере) получает метку времени . Точность этих меток должна быть достаточной, для того чтобы все метки времени были уникальными.

Каждому элементу данных ***x*** присваивается две метки времени:

* метка транзакции, записавшей последнее значение этого элемента  ***(x)***;
* метка последней транзакции, прочитавшей это значение  ***(x)***.

В реализации эти метки нужны только для элементов данных, которые обрабатываются активными транзакциями.

Протокол ***TS*** предусматривает следующие правила выполнения транзакций:

***TS-R*** Операция  ***(x)*** допустима, если ***(x) <*** , т. е. последняя запись элемента данных ***x*** была выполнена транзакцией, стартовавшей раньше, чем читающая транзакция. Если это условие не выполнено, то операция чтения отвергается и транзакция обрывается.

***TS-W***Операция записи  ***(x)*** допустима, если  ***(x)* <** , т. е. последнее чтение элемента данных было выполнено транзакцией, стартовавшей раньше, чем транзакция, записывающая новое значение. Если это условие нарушено, то операция отвергается и транзакция должна быть оборвана.

Протокол ***TS*** генерирует расписания, сериализуемые с сохранением порядка транзакций: ***Gen(TS) ⊂ OCSR***.

В протоколах, основанных на блокировках, нет необходимости специально заботиться об этом, потому что для этих протоколов необходимая синхронизация обеспечивается блокировками попутно с сериализуемостью

Для доказательства заметим, что правила протокола ***TS*** гарантируют, что направление конфликтов совпадает с их направлением в эквивалентном серийном расписании, в котором транзакции упорядочиваются по возрастанию их меток времени.

При реализации протокола ***TS*** необходимо гарантировать, что все операции над каждым элементом данных выполняются строго последовательно. Это может быть необходимо, если оборудование и операционная система допускают параллельное выполнение.

Для того чтобы выполнение операций над каждым элементом данных было последовательным, можно использовать блокировки, устанавливаемые на время выполнения одной операции. В некоторых системах блокировки, устанавливаемые на короткое время для предотвращения одновременной модификации разными процессами, называются задвижками ***(latch)***, в других этот термин применяется в более узком смысле (для конкретных типов объектов).

Такие блокировки устанавливаются только на один элемент данных, поэтому они могут устанавливаться локально даже в распределенных системах, не могут привести к ситуации тупика и никак не связаны с обеспечением сериализуемости (или другого уровня изоляции).

**Реализации протокола SI**

Любая реализация протокола **SI** должна обеспечить выполнение следующих двух требований:

1) возможность чтения значений данных, которые были зафиксированы на момент начала транзакции;

2) невозможность обновления одних и тех же данных конкурентно выполняемыми транзакциями.

Для реализации этих требований используются блокировки, устанавливаемые в соответствии со следующими правилами:

***SI1*** Используются только блокировки для операций записи.

***SI2***Транзакция, пытающаяся установить блокировку, несовместимую с блокировкой, установленной другой транзакцией, обрывается. Правило ***ﬁrst writer wins*** - побеждает первый записавший.

***SI3*** Изменения, сделанные транзакцией, становятся доступными для других транзакций во время ее фиксации (хранятся до ее завершения в отдельных областях памяти, недоступных другим транзакциям, которые в это время могут читать ранее зафиксированные копии элементов данных).

Использование блокировок в этом варианте протокола ***SI*** не связано с понятием конфликта, а только предотвращает одновременную модификацию элемента данных разными транзакциями. В соответствии с определением класса расписаний ***SI***, множества элементов данных, обновляемых одновременно выполняемыми транзакциями, не могут пересекаться.

В **многоверсионном** варианте протокола разные транзакции могут одновременно читать различные версии одного элемента данных.

Требования абстрактного протокола ***SI*** предполагают проверку интервалов времени, в течение которых выполняются транзакции, поэтому проверку этих условий легко реализовать на основе меток времени (подобно протоколу ***TS***) без применения блокировок.

**Многоверсионные протоколы**

Большинство протоколов управления транзакциями имеют варианты, работающие с множественными версиями элементов данных. Во всех случаях применение множественных версий сокращает долю транзакций, обрываемых по протокольным причинам: множественные версии дают возможность нормально зафиксировать транзакции, которые читают данные после того, как эти элементы данных были изменены логически более поздней транзакцией (т. е. более поздней в порядке сериализации). **Попытка записи таких элементов данных все равно приводит к обрыву транзакции.**

Наиболее просто множественные версии встраиваются в протокол **TS**: для каждой операции чтения выбирается последняя версия элемента данных, метка записи которой предшествует метке читающей транзакции. При этом для каждого элемента данных может потребоваться неограниченно большое количество версий, однако нет необходимости хранить версии, записанные раньше, чем последняя версия, записанная непосредственно до начала самой старой активной транзакции.

Если эта версия является последней для элемента данных (т. е. не была записана активной транзакцией) и если она не была прочитана ни одной из активных транзакций, то ее метки времени можно не хранить. Нет необходимости в хранении меток последнего чтения для всех версий, кроме последней записанной, т. к. попытка изменения любой версии, кроме последней, приводит к обрыву транзакции.

Проверка сериализуемости в многоверсионном варианте протокола ***TS*** использует не только метки времени записи, но и метки времени последнего чтения: **версия, прочитанная более поздней транзакцией, не может быть изменена более ранней, даже если это последняя записанная версия**.

В многоверсионном протоколе **SI** необходимо иметь возможность определять, какая именно версия каждого элемента данных должна быть доступна транзакции (входит в ее снимок состояния базы данных), и предотвращать доступ транзакции к другим версиям. По определению это последняя версия, записанная транзакцией, зафиксированной на момент старта транзакции, для которой строится снимок.

**Реализация может использовать либо метки времени,** связываемые с каждой версией и указывающие время фиксации транзакции, которая эту версию записала, **либо связывать с версией идентификатор записавшей транзакции** и при чтении проверять список транзакций, которые были активны на момент старта читающей.

Несколько сложнее **построить многоверсионные протоколы двухфазного блокирования**, потому что порядок сериализации может не совпадать с порядком, в котором транзакции выполнялись. Простую реализацию допускает двухверсионный двухфазный протокол, в котором для любого элемента данных необходимо хранить не более двух версий: последнюю зафиксированную и версию, обновляемую транзакцией, установившей блокировку на обновление.

**Такой протокол, однако, сохраняет большую часть недостатков одноверсионного 2PL.**

**Блокировки или метки времени**

**Основное назначение блокировок** – организовать выполнение операций разных транзакций в таком порядке, который обеспечивает выполнение некоторых условий корректности. **Ту же функцию выполняют и метки времени**, поэтому можно сказать, что блокировки и упорядочивание операций на основе меток времени в каком-то смысле взаимозаменяемы.

**Отличие состоит в том, что при невозможности немедленного выполнения операций** **блокировки приводят к ожиданиям, а применение меток времени — к обрывам транзакций**.

**Лекция 3. Надежность данных**

**1. Восстановление после отказов**

**Задача:** обеспечение сохранности данных, при этом данные должны оставаться в корректном состоянии.

**Категории отказов СУБД** :

* отказы транзакций и приложений;
* отказы сервера;
* разрушение носителей.

**2.1. Журнал транзакций**

1. Уникальный идентификатор LSN (log sequence number), тип **pg\_lsn**, 8 байтов – смещение записи от начала журнала.
2. Вариант формата: 4 байта - № файла журнала, 4 байта – смещение в файле.
3. Типы записей: BEGIN\*, COMMIT, ROLLBACK, UNDO\*, REDO, CHECKPOINT, создание резервных копий, файлов и др.

\* в PG не применяется.

**Записи заносятся в журнал строго последовательно**

**Правила ведения журнала (опережающая запись, write-ahead logging, WAL)**:

* **WAL1**: записи, регистрирующие любые изменения в БД, должны быть занесены в журнал и вытолкнуты на диск, до того как сами эти изменения (в БД) попадут на диск;
* **WAL2**: информация о фиксации транзакций в журнале должна быть вытолкнута на диск раньше, чем завершится операция фиксации, и раньше, чем приложение получит информацию о том, что фиксация выполнена успешно.

**Записи о модификации данных в журнале**

* **логические**: связанные с выполняемыми операциями SQL (INSERT, UPDATE, DELETE);
* **физические**: отражающие состояние измененных страниц БД.

В любом случае для каждой операции модификации могут быть созданы две записи: UNDO и REDO. Это дает возможность как устранить результаты выполнения операции, так и выполнить ее повторно.

**Стратегия записи в журнал**

* гарантирует возможность *восстановления* согласованного состояния базы данных;
* обеспечивают выполнение требований *атомарности и долговечности* транзакций: завершенные транзакции не могут быть потеряны, а оборванные (или не завершенные до отказа) транзакции не должны оставлять изменений в базе данных;
* задается свойствами:

**FORCE/NO FORCE**

**STEAL/NO STEAL**

FORCE означает, что все изменения, выполненные транзакцией, заносятся в БД и выталкиваются на диск до COMMIT.

NO FORCE означает, что записи REDO выталкиваются из журнала на диск до завершения фиксации, но не требуют записи изменений в базу данных.

Страницы (блоки) БД, содержащие изменения незафиксированных транзакций, могут выталкиваться на диск.

Запрещает выталкивание на диск страниц, содержащих изменения незавершенных транзакций.

**Возможные стратегии**

**1. FORCE + NO STEAL**

Все изменения записываются в БД в момент фиксации. Реализация методом теневых страниц. Для восстановления не требуются записи ни REDO, ни UNDO, поэтому при восст. после системных отказов журнал не нужен.

Менее эффективна при нормальной работе и в высоко-производительных системах не применяется.

**2. FORCE + STEAL**

Изменения должны быть записаны на диск БД до фиксации, могут возникать задержки при фиксации транзакций, выполнивших относительно большое количество изменений. Для этой стратегии не требуются записи REDO.

**Благодаря опережающей записи в журнал информация об изменениях не будет потеряна, даже если возникнет необходимость в рестарте сервера баз данных.**

**3. NO FORCE + NO STEAL**

Изменения записываются на диск БД только после фиксации транзакции. В этом случае записи UNDO не требуются.

Некоторые страницы, например, часто обновляемые различными транзакциями, могут слишком долго оставаться в оперативной памяти.

**4. NO FORCE + STEAL**

Полностью асинхронная запись изменений БД на диск, никак не связанная с фиксацией транзакций. Обычно именно эта стратегия используется высоко-производительными системами, в том числе PostgreSQL.

**2.2. Рестарт сервера**

После рестарта сервера база данных может оказаться в несогласованном состоянии!

**Алгоритм восстановления «Redo history»**

**1 фаза. Анализ и повторное выполнение**

Просмотр журнала в прямом направлении (от начала к концу) и повторное выполнение изменений операций всех транзакций, которые еще не были занесены в БД.

1. При обнаружении BEGIN транз. записывается в список активных транз. Если BEGIN не используются, то началом транз. является 1-я операция, помеченная идентификатором транз., который не встречался ранее.
2. Появление COMMIT приводит к исключению транзакции из списка активных.
3. REDO используются для повторения операций, если соотв. изменения еще не внесены в БД. Для того, чтобы определить, какие изменения занесены на страницу, на каждой странице имеется поле **PSN (page sequence number**), содержащее LSN посл.записи журнала, изменения которой уже есть на странице. Если LSN>PSN, то изменения заносятся на страницу и изменяется ее PSN.
4. Если изменение относится к активной транз., то изменяемый объект заносится в список объектов, измененных этой транз.

**2 фаза. Откат**

Просмотр журнала в обратном направлении (от конца к началу), и для всех операций из списка активных транзакций, полученного на первой фазе, выполняется операция отката с помощью записи UNDO. Операция отката регистрируется в журнале.

1. При обнаружении записи BEGIN для активной транзакции эта транзакция исключается из списка активных и выполняется ее фиксация, т. е. в журнал заносится запись COMMIT, и журнал выталкивается на диск.
2. Работа алгоритма заканчивается, когда список активных транзакций становится пустым.

Алгоритм восстановления после рестарта может быть **реентерабелен** - многократного выполнен (в случае отказа системы во время процедуры восстановления).

**2.3. Контрольные точки**

Механизм контрольных точек (КТ) предназначен для сокращения объема журнала, который просматривается при восстановлении.

Журнальная запись CHECKPOINT содержит **список активных транзакций и список страниц**, состояние которых в оперативной памяти отличается от состояния на диске.

После выталкивания записи о КТ фоновый процесс записи копирует все изменения из этого списка на диск. При этом нормальная работа системы продолжается.

Если при этом страницы, включенные в список, будут изменены новыми транзакциями, эти изменения попадут на диск. Изменения на страницах, не включенных в список, будут учтены в следующей контрольной точке.

Когда копирование страниц, включенных в КТ, заканчивается, в журнал заносится запись о завершении КТ.

**3. Разрушение носителя**

Для предотвращения потери данных в случае разрушения носителя, необходимо периодическое создание резервных копий.

Существует большое разнообразие методов создания резервных копий, различающихся :

* по сложности,
* полноте восстановления ,
* по стоимости.

1. **Простые** **методы** создания копий обеспечивают восстановление БД в состояние, которое было на момент создания резервной копии. При этом все изменения, выполненные после создания копии до отказа, будут потеряны.
2. Более **сложные методы** предполагают (в дополнение к копированию самой БД) хранение **журнала** транзакций. Для приведения системы в рабочее состояние после разрушения носителя необходимо восстановить БД с последней резервной копии и затем выполнить рестарт системы с использованием всех файлов журнала, записанных после создания этой резервной копии (а не с контрольной точки, как при отказе сервера).

**Основные метрики**, характеризующие качество процедур восстановления:

**Время восстановления.** Измеряется от начала процедуры восстановления до начала обработки новых транзакций. Время восстановления может варьироваться от нескольких часов для простых методов до долей секунды для сложных, и непосредственно влияет на характеристику доступности системы.

**Выживаемость.** Обозначает количество разрушений носителя, которое приводит к потере данных. Эта характеристика не обязательно совпадает с количеством копий, т. к. процедура восстановления может включать создание новой резервной копии, что делает ее более дорогостоящей и более продолжительной, но обеспечивает более высокую выживаемость.

**Задержка**. Время, необходимое для распространения изменений по резервным копиям, обеспечивающим выживаемость. Для простых методов, не использующих журнал, задержка равна интервалу между созданиями резервных копий. В высоконадежных системах задержка измеряется долями секунды.

**3.1. Экспорт и импорт**

**Экспорт** логической структуры БД в какой-либо внешний формат. В системе PostgreSQL такой экспорт можно выполнить с помощью утилиты **pg\_dump.**

**Недостатки**. Размещение данных после восстановления экспортированной БД, скорее всего, не будет совпадать с размещением в исходной БД, поэтому восстановление актуального состояния по журналу в этом случае невозможно.

Задержка может достигать значений, равных интервалу времени между созданиями резервных копий.

Применяется для БД , используемых только для разработки или тестирования приложений, когда система не находится в производственной эксплуатации или приложение является тиражируемым продуктом.

**3.2. Копирование с восстановлением по журналам**

Если допустимые значения задержки не должны превышать долей секунды, то методы на основе экспорта и импорта оказываются непригодными!

**Резервная копия** - точный образ БД, зачастую в формате, непригодном для непосредственного запуска сервера БД (возможно, в сжатом виде).

Для того чтобы использовать резервные копии, необходимо выполнить процедуру архивирования сегментов журнала, до того как они будут удалены.

**Дополнительно** необходимо сохранять все данные, записываемые при нормальной работе системы в журнал транзакций. (Сегменты журнала)

**Методы создания резервной БД**

• Применение программ создания резервных копий, входящих в состав СУБД. Для создания такой копии не требуется останавливать нормальную работу сервера БД.

• Копирование файлов БД (включая журнал транзакций) средствами ОС. Такое копирование может в некоторых системах работать быстрее, но для некоторых СУБД может требоваться остановка сервера БД, что влияет на доступность системы.

pg\_basebackup

Поскольку процедура восстановления предусматривает повторное внесение изменений по журналу в том порядке, в котором эти изменения выполнялись, возможно восстановление не только последнего согласованного состояния БД до момента отказа, но и состояния **на** **любой предшествующий момент** времени (после завершения записи резервной копии).

**3.3. Резервные серверы БД**

Большое время восстановления отрицательно влияет на характеристику доступности!

Для того чтобы исключить время копирования всей БД, резервные копии создаются в обычном формате БД и на этой копии запускается резервный сервер БД.

Создание и ведение таких серверов является одним из применений репликации БД.

Для применения любой схемы защиты от разрушений носителя с запасным сервером требуется не менее чем вдвое большая конфигурация оборудования (как минимум два сервера, каждый из которых обладает производительностью, достаточной для выполнения запросов прикладной системы в нормальном режиме работы).

**Лекция 4. Функции и процедуры в БД**

**1. Хранимые подпрограммы**

Возможности расширения функциональности системы **PostgreSQ**L в значительной мере основаны на механизме хранимых подпрограмм **(routines)**, определяемых пользователями.

В системе **PostgreSQL** имеются два вида таких подпрограмм: **функции** и **процедуры**.

Основное различие между ними состоит в том, что **функции возвращают результат**.

Для того чтобы функция была вызвана и выполнена, ее необходимо использовать в выражении в операторе SQL, например включить в список выражений, возвращаемых оператором SELECT. Процедуры не вырабатывают результат, а для вызова процедуры необходимо использовать оператор CALL.

Применения функций и процедур многообразны и включают как дополнение или изменение функций сервера баз данных, так и реализацию функциональности конкретных прикладных систем:

• реализация операций над пользовательскими типами данных;

• определение пользовательских агрегатов и оконных функций;

• определение триггеров;

• обеспечение разграничения доступа для пользователей приложений;

• реализация функций приложения, требующих интенсивной работы с базой данных.

• и д.р.

Хранимые процедуры и функции выполняются в рамках процессов сервера БД и поэтому могут выполняться более эффективно, чем код в программе-клиенте.

**+ нет необходимости в пересылке данных по сети**.

**– применение функций может существенно изменить поведение сервера баз данных (например, при массовом применении триггеров);**

**плохо продуманное использование функций, определенных пользователем, может фактически блокировать работу оптимизатора.**

**Негативные последствия применения функций и процедур могут возникать по следующим причинам:**

**Раздельное выполнение подзапросов.** Существенная часть работы оптимизатора запросов состоит в изменении порядка выполнения операций, указанных в запросе, например вложенные запросы могут преобразовываться в операцию соединения. Однако подзапрос, размещенный внутри функции, оптимизируется и выполняется отдельно от основного запроса, в котором использована функция.

**Побочные эффекты функций.** Возможности перестройки планов существенно сокращаются, если использованные в запросе функции не обладают некоторыми необходимыми свойствами, например изменяют состояние базы данных. **Недоступность оценок стоимости.** Если при определении функции не указаны параметры, описывающие стоимость ее выполнения, оптимизатор не может правильно оценить эту стоимость. Во многих случаях стоимость существенно зависит от значений параметров вызова функции, поэтому даже явное указание коэффициентов в определении функции оказывается не очень полезным.

Вызов функции всегда выполняется для некоторого запроса клиентского приложения, поэтому действие функции ограничено этим запросом, даже если внутри функции выполняется несколько операторов SQL или вызываются другие функции. **В теле функции нельзя использовать операторы управления транзакциями**.

В отличие от функций **процедуры вызываются** оператором **CALL** **и могут управлять транзакциями**, если только оператор вызова сам не находится внутри транзакции.

В отличие от методов объектов в традиционных языках программирования **функции (и процедуры) не могут сохранять никакие значения во внутренних переменных** между разными вызовами одной и той же или различных **функций**.

Зависимость результата выполнения функции от контекста описывается свойствами изменчивости.

• Функции с пометкой **IMMUTABLE** должны возвращать значения, зависящие только от их параметров, но не от содержимого БД или других значений (например, от времени), и не могут модифицировать БД.

• Функции, помеченные как **STABLE**, обязаны возвращать одни и те же значения при совпадающих значениях параметров и состояниях БД, но не могут зависеть от других значений и не могут модифицировать БД.

• Функции, для которых какие-либо из этих условий не выполнены, помечаются как **VOLATILE**. Если в запросе присутствуют такие функции, оптимизатор может применять только трансформации плана, не изменяющие контекст (параметры и состояние БД), в котором выполняются эти функции.

Если значения параметров такой функции известны на этапе планирования, она может быть вычислена планировщиком еще до выполнения запроса.

При определении STABLE подчеркивается, что одно и то же значение возвращается в пределах одного запроса. Если такая функция вызывается (с одинаковыми параметрами) несколько раз в одном запросе, оптимизатор может использовать результаты первого вызова вместо повторного выполнения функции.

Разницу в том, какие трансформации плана запроса, содержащего вызов функции, может применить оптимизатор, показано в примере: создадим функцию без параметров, возвращающую ложное значение, и проверим планы выполнения запросов с условием фильтрации, включающем вызов этой функции.

при пометке **VOLATILE** оптимизатор вынужден запланировать вызов функции для каждой строки результата:

**demo=# ALTER FUNCTION never VOLATILE; ALTER FUNCTION**

**demo=# EXPLAIN (costs off)**

**SELECT \* FROM aircrafts WHERE never(); QUERY PLAN**

**-------------------------------**

**Seq Scan on aircrafts\_data ml**

**Filter: never()**

Если функция создана с пометкой **IMMUTABLE**, фильтрация выполняется на этапе планирования и при выполнении запроса доступ к таблице не требуется:

**demo=# CREATE FUNCTION never() RETURNS boolean**

**LANGUAGE plpgsql IMMUTABLE AS $$**

**BEGIN**

**RETURN false;**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# EXPLAIN (costs off)**

**SELECT \* FROM aircrafts WHERE never();**

**QUERY PLAN**

**--------------------------**

**Result One-Time Filter: false**

При смене категории изменчивости на **STABLE** оптимизатор включает в план выполнения запроса доступ к таблице, но при фильтрации функция будет вызвана однократно:

**demo=# ALTER FUNCTION never STABLE;**

**ALTER FUNCTION**

**demo=# EXPLAIN (costs off)**

**SELECT \* FROM aircrafts WHERE never();**

**QUERY PLAN**

**-------------------------------------**

**Result**

**One-Time Filter: never()**

**-> Seq Scan on aircrafts\_data ml**

В системе PostgreSQL тело подпрограммы может быть записано на любом из языков программирования, известных серверу баз данных во время выполнения оператора, создающего функцию или процедуру.

Все функции и процедуры, независимо от того, на каком языке программирования они написаны, должны быть специфицированы оператором языка **SQL CREATE FUNCTION** или **CREATE PROCEDURE**.

Операторы **SQL CREATE FUNCTION** или **CREATE PROCEDURE** содержат тело функции или указание файла, из которого оно может быть загружено. Тело функции, если оно включено в оператор **CREATE**, записывается в виде константы, заключенной в кавычки. Кавычки могут быть необходимы и в теле функции; чтобы избежать их удваивания, целесообразно использовать именованные кавычки вида **$имя$**. Закрывающей кавычкой для нее становится только кавычка с таким же именем.

Функции и процедуры идентифицируются совокупностью, включающей:

1. имя функции;
2. имя схемы, в которой размещена функция;
3. количество и типы параметров.

Функции и процедуры, отличающиеся списком параметров, могут сосуществовать в одной схеме, что обеспечивает полиморфизм: при вызове функции выбирается та, которая имеет подходящие типы формальных параметров. Иногда этот вид полиморфизма называют перегрузкой (**overloading**).

При этом тип возвращаемого значения не является идентифицирующим, т. е. **функции, которые отличаются только типом возвращаемых значений, сосуществовать в одной схеме не могут.** Для изменения типа возвращаемого значения необходимо сначала удалить старое определение функции (оператором **DROP**).

Другая форма полиморфизма обеспечивается аппаратом **псевдотипов**. Если тип параметра функции задан псевдотипом, то в качестве значения такого параметра можно подставлять значение любого типа, соответствующего этому псевдотипу. Например, если параметр функции имеет тип **anyarray**, то значением такого параметра может быть **любой массив.**

**В системе PostgreSQL функции и процедуры вызываются из языка SQL, поэтому требуется преобразование** входных **аргументов подпрограммы** из типа данных SQL в тип данных языка программирования и обратное преобразование для выходных параметров и результатов.

**Исключение составляют подпрограммы, тело которых написано на SQL или на PL/pgSQL, потому что в этих языках применяется система типов SQL.**

Совокупность из двух функций, выполняющих такие преобразования, называется **трансформацией**. В обработчиках процедурных языков предусмотрены трансформации. Имеется возможность создать (оператором **CREATE TRANSFORM**) альтернативную, более эффективную трансформацию и задать ее в определении подпрограммы.

Аргументы функций могут быть **входными** (**IN**), **выходными** (**OUT**), **входными и выходными** (**INOUT**), а также **повторяемые** (**VARIADIC**). Выходные аргументы функций включаются в возвращаемый результат. Если выходных аргументов несколько, то они образуют кортеж, как в примере:

**demo=# CREATE FUNCTION get\_row (a int, b OUT int, c OUT int)**

**LANGUAGE plpgsql AS $$**

**BEGIN**

**b = a + 1;**

**c = a + 2;**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT get\_row(1);**

**get\_row**

**-----------------**

**(2,3)**

**(1 row)**

Фактические значения аргументов подпрограмм разделяются запятыми.

Их можно задавать позиционно (первое значение соответствует первому аргументу, второе — второму и т. д.), а также в формате *имя\_аргумента => значение*

В определении функции можно указывать значения аргументов, используемые по умолчанию.

Если такие значения заданы, то соответствующие параметры можно не указывать при вызове подпрограммы.

В процедурах не допускается указание выходных (**OUT**) аргументов, потому что процедуры не возвращают результат, однако допускаются аргументы **INOUT**, и, конечно, **IN** и **VARIADIC**.

Важная **особенность процедур** состоит в том, что, в отличие от функций, в них можно использовать операции управления транзакциями (такие как **START TRANSACTION, COMMIT, ROLLBACK**).

При определении подпрограмм можно задать новые значения параметров сервера БД, которые будут установлены на время выполнения этой подпрограммы. Таким способом можно задавать только те параметры, которые допускают динамическое изменение с помощью оператора **SET**.

После выхода из подпрограммы восстанавливаются значения параметров сервера, которые эти параметры имели перед входом в подпрограмму. Если такого указания в определении подпрограммы нет, но в теле использован оператор **SET**, то установленные этим оператором значения сохранятся и после выхода из подпрограммы.

Параметр **PARALLEL** определяет для оптимизатора возможность использования параллельных планов для запросов, содержащих определяемую функцию:

• **UNSAFE** указывает, что функцию можно использовать только в последовательных планах;

• **SAFE** указывает на возможность использования параллельных планов без ограничений;

• **RESTRICTED** ограничивает использование функции только головной (последовательной) частью параллельных планов.

**2. Процедурный язык PL/pgSQL**

Особое место PL/pgSQL среди многочисленных процедурных языков, поддерживаемых системой PostgreSQL, связано с тем, что этот язык очень хорошо интегрирован с SQL.

Непосредственным предшественником языка PL/pgSQL принято считать язык PL/SQL, применяемый в СУБД Oracle. По своему синтаксису оба эти языка относятся к семейству языков программирования, родоначальником которого можно считать Pascal, а другими представителями – Modula и Ada. Неформально, принадлежность к этому семейству выражается в том, что для выделения структурных единиц программного кода не используются фигурные скобки, как в языках программирования, входящих в семейство языка C.

**2.1 Структурные конструкции языка PL/pgSQL**

Тело любой функции, написанной на языке PL/pgSQL, оформляется как блок, содержащий:

1. необязательный раздел описаний локальных переменных, используемых в этом блоке (начинается ключевым словом **DECLARE**);
2. раздел, содержащий выполнимые операторы (начинается ключевым словом **BEGIN**);
3. необязательный раздел, описывающий обработку исключительных ситуаций (начинается ключевым словом **EXCEPTION**).

Весь блок завершается ключевым словом **END.** Все операторы, в том числе блоки, завершаются точкой с запятой.

Пример, близкий к минимальному:

**demo=# CREATE OR REPLACE FUNCTION hello(p text) RETURNS text**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**v text;**

**BEGIN**

**v := 'Hello, ';**

**RETURN v || p || '!';**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT hello('world');**

**hello**

**---------------**

**Hello, world!**

**(1 row)**

В языке PL/pgSQL можно использовать вложенные блоки и составные операторы, которые ограничивают области действия и области видимости локальных переменных. Условный оператор записывается в одной из следующих форм:

**IF условие THEN**

**оператор; ...**

**ELSE**

**оператор; ...**

**END IF;**

**IF условие THEN**

**оператор; ...**

**END IF;**

Оператор выбора альтернативных вариантов вычислений позволяет описывать ветвление на несколько альтернатив и может записываться в двух формах – с отдельными условиями на каждую альтернативу или с перечислением возможных значений выражения:

**CASE**

**WHEN условие - 1 THEN оператор; ...**

**WHEN условие - 2 THEN оператор; ...**

**...**

**ELSE**

**оператор; ...**

**END CASE;**

**CASE**

**WHEN условие - 1 THEN оператор; ...**

**WHEN условие - 2 THEN оператор; ...**

**...**

**ELSE**

**оператор; ...**

**END CASE;**

В языке определено большое количество различных вариантов оператора цикла. Тело цикла обрамляется ключевыми словами **LOOP** и **END LOOP**, между которыми размещается составной оператор:

**LOOP**

**оператор; ...**

**END LOOP;**

Количество повторений цикла определяется заголовком. В языке предусмотрены следующие варианты:

• **WHILE** *условие*

• **FO**R *переменная* **IN** *начало .. конец* **BY** *шаг*

• **FOREACH** *переменная* **IN ARRAY** *массив*

• Цикл без заголовка повторяется бесконечно

Для выхода из цикла можно использовать оператор **EXIT WHEN** условие. Этот оператор является **единственным способом выхода из цикла без заголовка.**

Оператор **CONTINUE** прекращает текущую итерацию цикла и выполняет переход к началу следующей итерации.

**2.2 Работа с объектами базы данных**

В качестве операторов в хранимых функциях и процедурах, написанных на языке PL/pgSQL, можно использовать операторы SQL. Если в выражениях, встречающихся в таком операторе, используются параметры функции или локальные переменные, то эти переменные подставляются как параметры подготовленного оператора SQL.

В действительности интерпретатор PL/pgSQL не вычисляет никакие выражения – вместо этого формируется неявный оператор SQL. Это, с одной стороны, гарантирует идентичность системы типов данных, с другой — приводит к появлению накладных расходов на формирование и обработку этих операторов.

Если оператор SQL возвращает одну строку, то значения, содержащиеся в этой строке, можно записать в переменные с помощью предложения **INTO**. Для оператора **SELECT** это предложение размещается сразу после списка выбираемых значений, для всех остальных операторов манипулирования данными (**INSERT, UPDATE, DELETE** с предложением **RETURNING**) – последним предложением, т. е. тоже после списка возвращаемых значений.

**demo=# CREATE OR REPLACE FUNCTION air\_city (a\_code text) RETURNS text**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**v text;**

**BEGIN**

**SELECT city**

**INTO v**

**FROM airports**

**WHERE airport\_code = a\_code;**

**RETURN v;**

**END;**

**$$; CREATE FUNCTION**

**demo=# SELECT air\_city ('SVO');**

**air\_city**

**----------**

**Москва (1 row)**

Если записать эту функцию на SQL (а не на PL/pgSQL), то код получится еще более компактным. Предложение **INTO** полезно в тех случаях, когда получаемые значения используются в других операторах в той же функции.

Если после ключевого слова **INTO** указано **STRICT**, то выполняемый оператор SQL должен возвращать ровно одну строку.

Количество строк результата выполнения любого оператора SQL (не важно, с предложением INTO или без него) можно узнать с помощью оператора

**GET CURRENT DIAGNOSTICS**. В частности, этот оператор можно использовать для получения значения **ROW\_COUNT** – количества строк, возвращенных последним запросом. Также, в каждой функции предопределена локальная переменная **FOUND** типа **boolean**, указывающая была ли выбрана (хотя бы одна) строка последним оператором SQL, который может возвращать строки.

Другой, более низкоуровневый способ обработки результатов запросов, возвращающих несколько строк, использует понятие ***курсора***, представляющего собой объект БД, содержащий частично выполненный запрос.

В языке PL/pgSQL для манипулирования курсорами используются переменные, параметры и результаты функций типа **refcurso**r. Для того чтобы начать работу с курсором, необходимо открыть его оператором **OPEN** (курсор можно явно закрыть оператором **CLOSE**)для выполнения запроса. **Открытый курсор можно возвращать как результат функции и принимать его в качестве параметра**.

Для получения данных из курсора используется оператор **FETCH**, а для изменения текущей позиции в множестве строк, составляющих результат выполнения запроса, применяется оператор **MOVE**. При завершении транзакции все открытые в ней курсоры закрываются автоматически.

Во многих языках программирования применение курсоров является единственным способом обработки результатов запросов.

Следующая функция демонстрирует использование курсора

**demo=# CREATE OR REPLACE FUNCTION plane\_set\_cur()**

**RETURNS SETOF airplane**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**cur refcursor;**

**v record;**

**BEGIN**

**OPEN cur FOR SELECT \* FROM aircrafts;**

**LOOP**

**FETCH NEXT FROM cur INTO v;**

**EXIT WHEN NOT FOUND;**

**RETURN NEXT ROW(v.aircraft\_code, v.model)::airplane;**

**END LOOP;**

**CLOSE cur;**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT \* FROM plane\_set\_cur();**

**code | model**

**------+---------------------**

**773 | Боинг 777-300**

**SU9 | Сухой Суперджет-100**

**320 | Аэробус A320-200**

**(3 rows)**

**2.3 Динамический SQL**

Операторы SQL можно формировать динамически как значения текстовых выражений. Такие операторы могут принимать параметры, значения которых передаются из переменных PL/pgSQL.

**demo=# CREATE OR REPLACE FUNCTION air\_city\_dyn(a\_code text)**

**RETURNS text**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**v text;**

**query\_text text :=**

**'SELECT city FROM airports WHERE airport\_code = $1';**

**BEGIN**

**EXECUTE query\_text**

**INTO v**

**USING a\_code;**

**RETURN v;**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT air\_city\_dyn('SVO');**

**air\_city\_dyn**

**------------------------**

**Москва**

**(1 row)**

Позиции в запросе, в которые необходимо подставить значения параметров, обозначаются псевдопеременными **$1, $2** и т. д. Для выполнения динамического SQL используется оператор **EXECUTE**. В нем предложение **USING** указывает переменные функции, которые надо подставить в SQL, а предложение **INTO**, как и в операторах SQL, указывает, куда поместить результаты.

Динамический SQL можно также использовать в заголовках циклов и в курсорах, например, можно задавать запрос в виде выражений, вырабатывающих текстовые строки:

**FOR v IN EXECUTE 'SELECT \* FROM aircrafts‘**

или

**OPEN cur FOR EXECUTE 'SELECT \* FROM aircrafts';**

Значения переменных PL/pgSQL можно передавать, преобразуя их в строковые константы или с помощью механизма **псевдопеременных $n**.

Последний способ предпочтительнее, т. к. предотвращает атаки путем внедрения SQL-кода, однако его можно применять только в тех случаях, когда в SQL необходимы значения атрибутов. Псевдопеременные нельзя использовать, например, для передачи имен таблиц или выражений. В таких случаях необходимо конкатенировать текстовые значения и, соответственно, принимать дополнительные меры для защиты от возможных атак, используя специальные функции.

• Функция **quote\_ident** представляет свой аргумент как правильно записанное имя идентификатора, при необходимости окружая значение двойными кавычками и удваивая встречающиеся внутри двойные кавычки.

• Функция **quote\_literal** возвращает значение своего аргумента как правильно записанную строковую константу в одиночных кавычках.

• Функция **quote\_nullable** работает как предыдущая, но если аргумент имеет значение **NULL**, то возвращается **строка «NULL»**

**Применение этих функций гарантирует, что значения переменных не будут рассматриваться как часть SQL-кода.**

**Попытка внедрения** приведет к тому, что будет сформирован некорректный оператор SQL, выполнение которого **вызовет ошибку**, или включаемый код будет превращен в текстовую константу.

**В том и другом случае включаемый злоумышленником код не будет выполнен.**

Альтернативный способ достижения тех же целей предоставляет функция **format**, похожая на функцию **sprintf** языка программирования C. Первый параметр этой функции задает формат, в который подставляются значения остальных параметров в соответствии с типом, указанным в формате. Следующий пример показывает, каким образом можно использовать типы «**I**» и «**L**», по своему действию эквивалентные функциям **quote\_ident** и **quote\_literal**:

**demo=# SELECT format(**

**'SELECT \* FROM %I WHERE name = %L',**

**'table name', 'a value‘**

**);**

**format**

**---------------------------------------------------**

**SELECT \* FROM "table name" WHERE name = 'a value‘**

**(1 row)**

**2.4 Обработка исключительных ситуаций**

Если при выполнении функции возникает исключительная ситуация, препятствующая продолжению работы, обычно выполнение функции прекращается и сообщение об ошибке возвращается клиенту. Однако если в блоке PL/pgSQL имеется раздел **EXCEPTION**, в котором предусмотрена обработка этой ситуации, то выполняются операторы этого обработчика, и затем выполнение блока может быть завершено нормально или аварийно в зависимости от обработчика ошибки.

При возникновении любой исключительной ситуации система PostgreSQL выполняет откат базы данных в то состояние, которое она имела в момент начала выполнения наименьшего блока, в котором предусмотрена обработка этой исключительной ситуации и внутри которого она возникла. Если такого блока нет, то выполняется откат транзакции, в которой возникла исключительная ситуация.

Тип ошибки задается предложением **WHEN** условие **THEN**, за которым следуют операторы, выполняющие обработку ошибки. В качестве условия может быть указано имя исключительной ситуации, условие на код ошибки или ключевое слово **OTHERS** для обработки всех ситуаций, не предусмотренных для предшествующих обработчиков в этом блоке.

**Пример исключительной ситуации:**

**demo=# CREATE OR REPLACE FUNCTION air\_city(a\_code text) RETURNS text**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**v text;**

**BEGIN**

**SELECT city**

**INTO STRICT v**

**FROM airports**

**WHERE airport\_code = a\_code;**

**RETURN v;**

**EXCEPTION**

**WHEN no\_data\_found THEN**

**RETURN '-- Invalid airport code --';**

**WHEN OTHERS THEN**

**RAISE;**

**END;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT air\_city('XXX');**

**air\_city**

**----------------------------------------------------**

**Invalid airport code --**

**(1 row)**

В этом примере в предложении **INTO** добавлено ключевое слово **STRICT**, требующее, чтобы в результате выполнения запроса была найдена ровно одна строка. Поскольку в вызове функции указан неверный код аэропорта, возникает исключительная ситуация, предусмотренная первым обработчиком, который возвращает константу и завершает функцию нормально.

Конечно, такой возврат сообщения об ошибке вместо результата нельзя считать хорошим стилем программирования.

Второй обработчик возбуждается при возникновении любой другой ошибки и возбуждает ту же самую ошибку оператором **RAISE**. Такой обработчик не имеет никакого смысла, потому что он стирает информацию о том, где в действительности произошла ошибка (которая могла произойти в любой функции, вызываемой из блока, где находится обработчик ошибок).

При обработке исключительных ситуаций можно использовать предопределенные переменные **SQLSTATE** (код ошибки) и **SQLERRM** (сообщение об ошибке). Можно получить более детальную информацию с помощью оператора **GET STACKED DIAGNOSTICS**. Оператор **RAISE** позволяет выводить информационные сообщения, а также возбуждать исключительные ситуации, в том числе определенные пользователем. В предыдущем примере такой же результат можно получить, проверяя наличие строк в ответе на запрос вместо применения ключевого слова **STRICT:**

**demo=# CREATE OR REPLACE FUNCTION air\_city(a\_code text) RETURNS text**

**LANGUAGE plpgsql AS $$**

**DECLARE**

**v text;**

**BEGIN**

**SELECT city**

**INTO v**

**FROM airports**

**WHERE airport\_code = a\_code;**

**IF NOT FOUND THEN**

**RETURN '-- Invalid airport code --';**

**END IF;**

**RETURN v;**

**END;**

**$$;**

Можно сформулировать несколько рекомендаций по применению средств обработки исключительных ситуаций, которые имеет смысл учитывать при проектировании прикладной системы, использующей хранимые подпрограммы.

• При обработке исключительных ситуаций необходимо сохранять системную диагностику, для того чтобы облегчить выявление причин, вызвавших возбуждение такой ситуации.

• Обработка исключительных ситуаций необходима, для того чтобы скрыть от конечного пользователя системные сообщения об ошибках.

• Целесообразно включать обработку исключительных ситуаций в подпрограммы, которые выполняются как часть одного тяжеловесного процесса, состоящего из нескольких относительно независимых частей.

• Целесообразно включать обработку исключительных ситуаций в тех случаях, когда вероятность возникновения исключительной ситуации относительно велика.

Обработчики исключительных ситуаций, в отличие от основного выполняемого кода, могут перехватывать ошибки, возникающие не только в блоке, в котором размещен обработчик, но и в любом динамически вложенном, в том числе в других функциях, выполнение которых инициировано из этого блока.

Поэтому обычно нецелесообразно обрабатывать исключительные ситуации в подпрограммах, которые вызываются из подпрограмм, где такая обработка уже предусмотрена.

Целесообразно обрабатывать исключительные ситуации на том уровне, где такая обработка может дать диагностику, которую легко интерпретировать в терминах приложения. Если же такая диагностика невозможно, то, вероятно, лучше вовсе не перехватывать ошибки.

**3. Функции и процедуры на языке SQL**

Тело функции или процедуры на языке SQL, представляет собой последовательность операторов SQL, разделенных «;». Последний оператор формирует результат функции. Если результат функции специфицирован не как таблица (**TABLE** или **SETOF**), то возвращается первая строка результата последнего оператора. Примеры записи функций на языке SQL:

**1)** Функция, возвращающая одно скалярное значение:

**demo=# CREATE OR REPLACE FUNCTION hello(p text) RETURNS text**

**LANGUAGE sql AS $$**

**SELECT 'Hello, ' || p || '!';**

**$$;**

**CREATE FUNCTION**

**demo=# select hello('world');**

**hello**

**---------------------**

**Hello, world!**

**(1 row)**

**2)** Функция, возвращающая множество строк составного типа:

**demo=# CREATE OR REPLACE FUNCTION plane\_set() RETURNS SETOF airplane**

**LANGUAGE sql AS $$**

**SELECT ROW(aircraft\_code, model)::airplane**

**FROM aircrafts;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT \* FROM plane\_set();**

**code | model**

**-------+---------------------**

**773 | Боинг 777-300**

**763 | Боинг 767-300**

**SU9 | Сухой Суперджет-100**

**(3 rows)**

Если в спецификации функции на языке SQL нет указания **SETOF** (или **TABLE**), то функция возвращает первую строку результата:

**demo=# CREATE OR REPLACE FUNCTION plane\_row() RETURNS airplane**

**LANGUAGE sql AS $$**

**SELECT ROW(aircraft\_code, model)::airplane**

**FROM aircrafts;**

**$$;**

**CREATE FUNCTION**

**demo=# SELECT \* FROM plane\_row();**

**code | model**

**-----------+--------------------------**

**773 | Боинг 777-300**

**(1 row)**

Применение функций, написанных на языке SQL, предоставляет возможность для вынесения запросов из кода приложения, а также может быть полезно как инструмент ограничения доступа, однако некоторые виды функций, например **функции триггеров, на SQL писать нельзя.**

Важная особенность функций на языке SQL состоит в том, что в ряде случаев оптимизатор может подставлять тела таких функции в запрос, в котором они вызываются. Для этого функция должна содержать единственный оператор **SELECT** и должна быть объявлена как **SECURITY INVOKE**R. Кроме того, функция, возвращающая множество строк, должна быть объявлена как **STABLE** или **IMMUTABLE**, а скалярным функциям нельзя обращаться к таблицам и содержать предложения **FROM**, **GROUP BY**, **ORDER BY** и т. п.

**Лекция 5. Мониторинг баз данных**

**1.1. Основы мониторинга**

Администратор должен проводить регулярный **мониторинг**

1. пользователей базы;
2. активности клиентских сеансов;
3. используемых ресурсов.

Составление расписания выполнения разного рода регулярных задач, например процедур извлечения, преобразования и загрузки данных (**extract-transform-load, ETL**) в хранилище данных для последующей аналитической обработки.

Регулярный мониторинг позволяет **уловить моменты**, когда в системе

1. внезапно увеличивается потребление процессорного времени или операций ввода-вывода, или
2. значительно возрастает количество соединений.

Администратор сможет вовремя определить угрозу исчерпания выделенных ресурсов.

Мониторинг **активности клиентских сеансов:**

1. многочисленные системные представления и
2. специальные статистические функции, которые по своему назначению могут быть разбиты на две группы.

**1-я группа** ориентирована на получение оперативной информации о том,

что только что произошло или происходит в базе.

**2-я группа** – на получение общих сведений о работе, размерах базы и статистической информации с момента ее последнего сбора.

Системное представление **pg\_stat\_activity** относится к первой группе и может быть использовано для получения системного идентификатора серверного процесса, сведений о подключении, времени начала выполнения активного в данный момент запроса и текста этого запроса, текущего события ожидания процесса и другой информации.

**Динамика** работы с базой отражается в нескольких системных представлениях.

**pg\_stat\_database** отражает

1. динамику изменения баз с момента предыдущего сбора статистики,
2. количество зафиксированных и оборванных транзакций,
3. сведения об интенсивности доступа к данных (как в строках, как и в страницах) и много другой полезной информации.

Имена баз данных и количество добавленных, измененных и удаленных строк в этих базах:

SELECT datname, tup\_inserted, tup\_updated, tup\_deleted

FROM pg\_stat\_database;

Статистику по различным объектам баз данных можно увидеть в таких представлениях, как

pg\_stat\_user\_tables,

pg\_stat\_user\_indexes,

pg\_stat\_user\_functions.

Использование системного представления **pg\_class** для вывода информации о размерах (в страницах) десяти самых больших таблиц демонстрационной базы данных:

demo=# SELECT relname, relpages

FROM pg\_class

ORDER BY relpages DESC

LIMIT 10;

Действительный **размер отношений** можно смотреть функциями **pg\_relation\_size** или **pg\_total\_relation\_size** (последний вариант включает для таблиц размер всех индексов и данных, вынесенных в таблицы TOAST).

Похожие функции есть и для баз данных (**pg\_database\_size**), и для табличных пространств (**pg\_tablespace\_size**)

**1.2. Настройка производительности**

**Настройкой** называется комплекс мер по приведению прикладной системы в соответствие с требованиями производительности без изменения ее функциональности.

**Исходные данные** для настройки :

Мониторинг

1. размеры хранимых объектов;
2. как данные используются (какие запросы выполняются и с какой частотой, какие данные с наибольшей вероятностью будут использоваться, как будет происходить ввод данных, с какой скоростью будут расти предполагаемые объемы данных и т. п.)
3. настройка **серверов приложений** и серверов баз данных (конфигурирование серверов и установка подходящих параметров);
4. настройка **схемы** базы данных (например, создание дополнительных индексов для более эффективного выполнения некоторых запросов, материализация «тяжелых» представлений, секционирование больших таблиц и т. п.);
5. локальная настройка отдельных **функций или запросов** (изменение кода отдельных запросов или функций приложения)

Если хорошо настроенные запросы потребляют значительную долю ресурсов сервера, то ничто, кроме увеличения мощности оборудования, не может улучшить производительность.

**1.3. Настройка серверов БД PostgreSQL**

Настройка сервера выполняется с помощью **параметров**, которые могут задаваться в конфигурационных файлах системы PostgreSQL.

**1. Управление оперативной памятью**.

Эти параметры задают размеры различных областей памяти, которые могут использоваться для кеширования базы данных (shared\_buffers), для хранения временных данных каждого сеанса (temp\_buffers), для хранения промежуточных данных при выполнении отдельных запросов и операций (work\_mem, maintenance\_work\_mem)

**2. Управление дисковым хранилищем.**

Размещение постоянно хранимых данных определяется с помощью табличных пространств, а параметр сервера позволяет ограничить размер выделяемой области для временно хранимых служебных данных, например для промежуточных результатов операций, если эти результаты не помещаются в выделенной области оперативной памяти (temp\_file\_limit).

**3. Управление фоновыми процессами.**

Фоновые процессы выполняют достаточно разнообразные действия, в том числе очистку и уплотнение данных (сборку мусора, vacuum), запись контрольных точек, сбор статистических характеристик хранимых данных. Частота запуска и другие особенности выполнения этих процедур влияют на загруженность системы и, таким образом, на ее производительность. Как правило, каждый фоновый процесс настраивается собственным набором конфигурационных параметров (количество которых может достигать нескольких десятков).

**4. Управление оптимизатором.**

Параметры, относящиеся к этой группе, могут наиболее существенно повлиять на производительность.

**Функция стоимости**, используемая оптимизатором, представляет собой линейную комбинацию нескольких критериев, учитывающих стоимость различных ресурсов.

Относительная стоимость ресурсов, необходимых для выполнения запроса, задается конфигурационными параметрами

При использовании SSD стоимости различных видов операций обмена отличаются не так существенно. В этом случае значение параметра random\_page\_cost следует уменьшить

Доступ к произвольным блокам (**random\_page\_cost**) на вращающихся дисках обычно в десятки раз медленнее, чем последовательный просмотр нескольких соседних блоков (**seq\_page\_cost**) на том же устройстве. Это соотношение, однако, может оказаться значительно меньше, если существенная часть базы данных находится в буферах в оперативной памяти; поэтому в своих оценках оптимизатор также учитывает оценку памяти, отведенной под кеш (как на уровне СУБД, так и в операционной системе, **effective\_cache\_size**).

Другая группа параметров влияет на конфигурацию **пространства планов**, которые будут рассматриваться оптимизатором при поиске оптимального плана.

С помощью этих параметров можно исключить из рассмотрения планы, содержащие определенные виды физических операций.

Для операций **фильтрации хранимых таблиц** параметры дают возможность исключать полный просмотр таблиц (**enable\_seqscan**), использование индексного просмотра (**enable\_indexscan**), построение и сканирование битовых карт, полезное в том числе при наличии нескольких условий фильтрации, поддержанных индексами (**enable\_bitmapscan**), а также чтение данных только из индексов (**enable\_indexonlyscan**).

Для двуместных операций можно запретить оптимизатору использование каждого из классов алгоритмов: хеширования (**enable\_hashjoin**), вложенных циклов (**enable\_nestloop**) и сортировки на основе слияния (**enable\_mergejoin**).

Параметры, определяющие пороговые значения количества операций соединения (**join\_collapse\_limit**) или вложенных подзапросов (**from\_collapse\_limit**), по достижении которых оптимизатор прекращает исчерпывающий просмотр пространства планов.

Еще один параметр(**geqo\_threshold**) определяет пороговое значение количества соединений, включающее стохастический метод поиска оптимального плана (генетический алгоритм).

**1.4. Настройка схемы БД**

Создание **индексов**

Для грамотного выбора набора создаваемых индексов необходимо знание особенностей приложения и требований к нему, характеристик нагрузки на БД (набора частот появления различных запросов), а также особенностей реализации индексов и оптимизатора конкретной СУБД.

После создания индекса необходимо проверить:

1. действительно ли он используется при выполнении тех запросов, для ускорения которых создавался, и действительно ли такое ускорение происходит.
2. что создание индекса не привело к ухудшению планов других запросов.

Другим методом настройки схемы является создание **материализованных представлений**.

В отличие от индексов материализованное представление необходимо явно указывать в запросе, чтобы оно было использовано.

Применение материализованных представлений особенно **целесообразно**, если выполняются следующие условия:

1) запрос, определяющий материализованное представление, выполняет вычисления, результаты которых часто используются в запросах;

2) семантика приложения допускает использование устаревших значений.

Методы и приемы, связанные с **размещением данных**. Этот довольно разнородный класс методов включает как управление размещением на физическом уровне (т. е. не затрагивает логику работы запросов и приложений), так и на логическом (требует модификации запросов).

**Табличные пространства**. Размещение хранимых объектов (таких как таблицы, индексы, материализованные представления и т. п.) может быть полезно для достижения весьма разнообразного набора целей.

1. часто используемые данные целесообразно размещать на более эффективных устройствах;
2. размещать файлы таблиц и индексы в разных табличных пространствах;
3. размещать так, чтобы данные, которые часто нужны в одном запросе, оказались на разных устройствах;
4. применять различающиеся стратегии создания резервных копий;
5. размещение объектов БД в нескольких табличных пространствах позволяет сократить количество файлов в одном каталоге ОС.

**Вертикальная фрагментация.**

**Горизонтальная фрагментация.**

**Нормализация.**

**Денормализация.**

**Изменение порядка колонок.**

**1.5. Настройка запросов**

Наиболее частой причиной низкой производительности оказывается **неэффективный код** самого запроса.

Перечень типичных ошибок:

1. Использование представлений, в которых содержатся соединения с таблицами, ненужными в рассматриваемом запросе.
2. Выборка значений первичного ключа из таблицы, соединение с которой выполняется по внешнему ключу. В этом случае операция соединения вообще не нужна, если из этой таблицы не выбираются другие колонки
3. Использование регулярных выражений для проверки условий, которые могут быть проверены по значениям других атрибутов.

**2. Надежность и доступность**

Доступностью (availability) называют отношение времени, в течение которого система была в работоспособном состоянии, т. е. принимала и выполняла запросы пользователей, к общему (календарному) времени.

Надежность системы определяется тем, насколько малы шансы потери данных.

Количественно для оценки надежности можно использовать две характеристики:

1. выживаемость, которая определяется как количество копий данных, которые должны быть разрушены, для того чтобы потеря данных произошла, и
2. время, необходимое, для того чтобы изменения или новые данные попали в резервные копии.

Выбор **стратегии** резервного копирования должен быть основан на реалистическом анализе потери данных и возможных последствий такой потери.

Стратегии обеспечения надежности и доступности **взаимосвязаны**. При отказе системы продолжительность восстановления влияет на доступность. Важно отметить, что **надежность** хранения связана также с **политиками обеспечения**

**безопасности**:

* все копии данных, из которых можно восстановить состояние основной БД, должны быть защищены по крайней мере в такой же степени, как основное хранилище.

**Недостаточно** просто регулярно создавать резервные копии базы.

**Полноценная** стратегия резервного копирования и восстановления должна быть хорошо документирована и включать:

• периодичность выполнения резервного копирования;

• время запуска регулярного резервного копирования;

• список лиц, допущенных к выполнению резервного копирования и востановления;

• объекты БД, подлежащие регулярному резервному копированию;

• точное указание места, где будут храниться резервные копии;

• сценарий выполнения резервного копирования;

• сценарий восстановления БД из резервной копии;

• периодичность пересмотра стратегии резервного копирования и восстановления БД.

**Доступностью** (availability) называют отношение времени, в течение которого система была в работоспособном состоянии, т. е. принимала и выполняла запросы пользователей, к общему (календарному) времени.

**Надежность** системы определяется тем, насколько малы шансы потери данных.

Количественно для оценки надежности можно использовать две характеристики:

1. **выживаемость**, которая определяется как количество копий данных, которые должны быть разрушены, для того чтобы потеря данных произошла, и
2. **время**, необходимое, для того чтобы изменения или новые данные попали в резервные копии.

**3. Репликация  
3.1. Множественные копии данных**

В случае баз данных дублирование сводится к организации хранения нескольких копий логически одних и тех же данных.

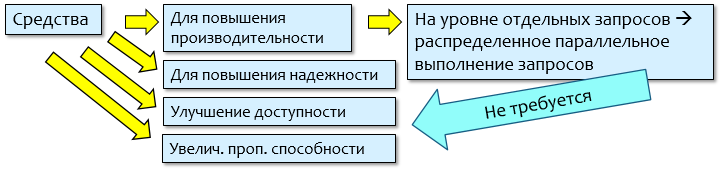
**Репликация**

Требуются **избыточные ресурсы**, использование которых позволяет улучшить ряд характеристик системы:

• надежность — данные не будут потеряны при разрушении части копий;

• доступность— обработка будет возможна, даже если некоторые копии временно недоступны;

• производительность — одновременная работа нескольких ресурсов может обслужить большее количество запросов или ускорить выполнение отдельных запросов.



**3.2. Согласованность реплик**

В идеале репликация должна быть **прозрачной**, т. е. результаты, получаемые пользователем, не должны зависеть от того, какие копии данных были использованы для получения этого результата.

Другими словами, поведение БД, для которой применяется репликация, с точки зрения приложений (и пользователей) не должно отличаться от поведения одной **централизованной** БД.

Понятие согласованности реплик отличается от понятия согласованности, которое основано на предположении об атомарности операций чтения и записи данных и при конкурентном обновлении обеспечивает корректность данных. (Абстрактная согласованность)

В системах с репликацией операции записи не могут считаться атомарными, поскольку значения каждого элемента данных хранятся на нескольких серверах. Поэтому понятие *согласованности реплик* дополняет понятие *абстрактной согласованности*.

|  |  |
| --- | --- |
| Обеспечивает глобальную согласованность данных, но его буквальная реализация (поддержка идентичности всех реплик) оказывается ресурсоемкой, может ограничивать доступность и ухудшать характеристики производительности системы. | Требование единой логической копии |

**Ослабление требования**: до каждой транзакции отдельно.

Тогда **для реализации** требуется только согласованность реплик, участвующих в выполнении транзакции (а не полная идентичность всех реплик)

Реализация требования может оказаться неустойчивой к разделению сети, т. е. к потере связи с частью реплик.

Если ни распределенные запросы, ни распределенные транзакции в системе не используются, то требование единой логической копии можно ослабить, заменив его на требование **локальной согласованности** всех реплик.

Правила обновления и распространения изменений по репликам.

Для поддержки требования единой логической копии необходимо все изменения выполнять одновременно на всех репликах.

Для ослабленного варианта требования единой логической копии существуют протоколы (симметричные), устойчивые к разделению сети и обеспечивающие очень высокую доступность на чтение.

Локальная согласованность полезна в сценариях, в которых оперативная работа выполняется на одной копии или на ограниченном количестве копий, а остальные используются для аналитической обработки

**3.3. Согласованность, доступность, разделение сети**

1. Точное определение того, как понимается **доступность**, может различаться в зависимости от класса систем и даже от типа выполняемых действий.

2. Термин «**согласованность**» также используется в различных смыслах.

Применительно к базам данных необходимо различать доступность для чтения и доступность для обновления данных.

Доказана «**теорема CAP**», утверждающая, что невозможно получить распределенную систему,

1. устойчивую к разделению вычислительной сети и
2. обладающую высокой доступностью и
3. обеспечивающую согласованность

Современные технологии СУБД обеспечивают возможность создания высокопроизводительных и высокодоступных распределенных баз данных, способных обрабатывать миллионы транзакций в секунду, не жертвуя при этом согласованностью.

**3.4. Поддержка единой логической копии**

Необходимо, чтобы все изменения, вносимые в БД, выполнять **одновременно** на всех копиях, или, более точно, изменения, вносимые любой транзакцией, должны быть выполнены на всех серверах до того, как эта транзакция будет зафиксирована.

**Глобальные транзакции**. Все транзакции сериализуются в рамках одного расписания, например, используются глобальные блокировки.

**Главная копия**. Все обновляющие транзакции выполняются на одном сервере, и внесенные ими изменения распространяются на все остальные копии. После этого обновляющие транзакции могут быть зафиксированы.

Не может обеспечить высокую доступность **для обновлений**, потому что отказ любого из серверов приводит к невозможности выполнения каких-либо обновлений во всей системе.

Требование одной копии при этом выполняется, и высокая доступность **по чтению** обеспечивается.

**3.4. Симметричные протоколы синхронизации реплик**

Чтобы увеличить доступность **при обновлении**, был предложен мажоритарный протокол, позволяющий выполнять обновляющие транзакции при частичной недоступности копий.

1. Значение элемента, подлежащего обновлению, считывается со всех доступных копий. Если количество считанных копий меньше чем S=S/2+1, то

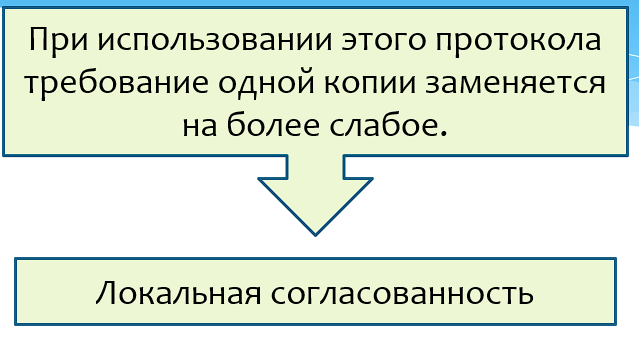
обновление невозможно и транзакция обрывается.

2. Из всех полученных значений выбирается самая последняя версия, и выполняется ее обновление в соответствии с запросом приложения.

3. Новая версия элемента распространяется на все доступные серверы.

Если серверу не доступно достаточное для обновления количество копий, он может тем не менее выполнять запросы на чтение, возвращая те версии данных, которые на нем имеются. Поэтому мажоритарный протокол может обеспечить **высокую доступность** при неустойчивой работе вычислительных сетей.

Любой сервер должен предоставлять согласованное состояние данных, но, возможно, **несколько устаревшее**, т. е. не учитывающее часть транзакций, выполненных на других серверах.



Общее количество копий – *S*.

Обновление выполняется только в том случае, если количество копий, доступных для обновляющего сервера, составляет не менее S=S/2+1.

**3.6. Репликация главной копии**

Наиболее часто используется организация репликации, при которой изменения могут выполняться только на **одном главном** (primary) сервере.

Изменения, выполненные на этом сервере, переносятся на все копии, которые могут использоваться только для чтения данных и называются запасными (standby) или репликами (replica).

Такие методы репликации не могут обеспечить доступность для модификации выше, чем доступность централизованной БД. Доступность на чтение может быть весьма высокой, если чтение устаревших копий допустимо.

Методы распространения обновлений с главного сервера на запасной

При ***синхронном распространении*** все изменения, выполненные на главном сервере, повторяются на запасных и должны быть завершены до того, как будет зафиксирована транзакция, выполнившая эти изменения на главном сервере.

При ***асинхронном распространении*** обновлений влияние репликации на основной сервер будет значительно меньше, но состояние БД на запасных серверах будет повторять состояние главного с некоторой задержкой.

Распространение обновлений можно выполнять на различных уровнях абстракции данных.

**Повторение операторов SQL**. В этом случае запасной сервер будет фактически повторять всю работу, которая выполняется на главном. Этот метод применяется крайне редко.

**Обновление логических записей**. При использовании этого метода обновления пересылаются в виде операторов SQL, каждый из которых обновляет ровно одну логическую запись (например, строку таблицы) по ее уникальному идентификатору. Как правило, в этом случае нагрузка на запасной сервер значительно ниже, чем в предыдущем, однако массовые операции обновления на основном сервере приводят к генерации очень большого количества обновлений отдельных записей. Выполнение этих операторов может занимать очень большое время.

**Распространение на уровне страниц БД**. При копировании физических страниц БД нагрузка на запасной сервер снижается до минимума, поскольку нет необходимости не только в синтаксическом разборе и выполнении операторов SQL, но и в какой-либо модификации страниц,

Поступающих с главного сервера. Более того , при таком распространении объем работы, выполняемый на запасном сервере, не может превосходить объем работы, выполненный на главном, поэтому операторы массового обновления никаких проблем не создают.

**Распространение записей журнала.** Этот вариант используется средствами репликации PostgreSQL. По своим характеристикам он близок к предыдущему. Отличие в том, что в этом случае страницы не копируются полностью, если они не содержатся в журнальных записях. Вместо этого используются записи REDO, как при восстановлении после отказа.

Основные случаи, в которых применяется репликация по схеме с одним главным сервером:

1. Создание копий, отражающих состояние БД на основном сервере на некоторый момент времени без последующего распространения изменений;
2. Снижение нагрузки на главный сервер и повышение производительности системы за счет переноса только читающих приложений на запасные серверы;
3. Распределение запросов в зависимости от типов нагрузки: все обновляющие запросы и запросы типа OLTP выполняются на одном сервере, а аналитические запросы типа OLAP — на другом или на других;
4. Создание резервных копий БД для использования в качестве главной копии в случае отказа основного сервера или разрушения носителя данных на нем.

**3.7. Резервные серверы БД**

Часто упоминаемым требованием к **высокодоступным системам** считается «пять девяток», т. е. 0,99999 или 99,999%. Такая доступность означает, что суммарное время недоступности системы в течение года не превышает 316 секунд за год или 6 секунд в неделю.

Схема репликации с главным сервером вполне подходит для создания резервных копий, поскольку в этом случае все изменения распространяются в одном направлении. На запасном оборудовании запускается сервер БД с включенным режимом восстановления по журналу (как при восстановлении после разрушений носителя данных). По мере создания новых архивированных сегментов журнала содержащиеся в них изменения повторяются на запасном сервере.

В случае **отказа** основного сервера на запасном обрабатывается последний файл журнала и после этого он переводится в режим основного сервера.

Запасной сервер в такой конфигурации называется сервером теплого резерва (**warm standby**).

Для того чтобы применять такую схему, необходимо, чтобы файлы журнала основного сервера были **доступны** даже в случае его отказа. Для этого файлы журнала записываются в нескольких копиях, размещенных на разных вычислительных системах.

В системе **PostgreSQL** (и в других высокопроизводительных системах) поддерживается и другая конфигурация, которая называется сервером в горячем резерве **(hotstandby**).

В этой конфигурации запасной сервер устанавливает соединение с основным (как клиент) и получает поток сообщений с информацией об изменениях, выполняемых в БД основным сервером.

Эти изменения практически немедленно (но асинхронно) выполняются и на запасном.

**3.8. Репликация в системе PostgreSQL**

1. **pg\_dump**
2. **pg\_dumpall**

Не репликация:

1. Согласованные копии в различных форматах, допускают полное или частичное копирование кластера, БД или отдельных схем.
2. Копирование выполняется на логическом уровне (выгруженные данные можно использовать для загрузки на сервер другой конфигурации)
3. Устанавливают соединение с сервером БД как обычные клиенты и не накладывают никаких ограничений на конфигурацию сервера.
4. Созданные копии не подлежат использованию в качестве запасных, поскольку они не предназначены для распространения изменений, внесенных в БД после создания копии.

**Репликация**

Программа pg\_basebackup создает копию кластера БД

Несколько различных способов организации автоматического распространения изменений с главного сервера на запасные

Один из них основан на передаче файлов (сегментов) журнала

Получение копий сегментов журнала с помощью программы **pg\_receivewal**, которая не дожидается заполнения сегмента, а получает поток записей журнала, устанавливая соединение с главным сервером

Включить режим **непрерывного архивирования**:

1. при переключении сегментов журнала регистрации изменений вызывается процедура архивирования только что законченного сегмента;
2. процедура должна сохранить данные из сегмента журнала, например просто скопировать его в другую файловую систему, в которой эти файлы накапливаются.

Для нормальной работы репликации с распространением обновлений необходимо, чтобы после создания копии с помощью **pg\_basebackup** все записанные (архивированные) файлы журнала оставались доступными.

Значительно меньшее отставание может обеспечить непосредственная связь между серверами. Возможны различные конфигурации запасного сервера.

Запасной сервер создает **сеанс работы с главным сервером**, в рамках которого запрашивает записи журнала главного сервера и обрабатывает их немедленно или с некоторой задержкой.

**Синхронная работа** главного и подчиненного серверов. Как и в предыдущем варианте, запасной сервер создает сеанс связи с главным, но если запасной сервер включен в список синхронных, то главный сервер выполняет передачу изменений в рамках транзакции, которая выполнила эти изменения. При этом транзакция фиксируется, но ее завершение задерживается до получения подтверждения с запасного сервера

**Лекция 6. Оценка соответствия и сертификация средств защиты информации**

В области ИБ существует несколько видов деятельности по оценке соответствия. К ним относятся:

– сертификация средств защиты информации;

– аттестация объектов информатизации;

– аккредитация органов, лабораторий, центров;

– различные виды испытаний и контроля;

– аудит безопасности программных средств, информационных систем и систем менеджмента информационной безопасности.

В соответствии с Федеральным законом "О лицензировании отдельных видов деятельности": **лицензирование** – деятельность лицензирующих органов:

– по предоставлению;

– переоформлению лицензий;

– продлению срока действия лицензий в случая;

– осуществлению лицензионного контроля;

– приостановлению;

– возобновлению;

– прекращению действия;

– аннулированию лицензий;

– формированию и ведению реестра лицензий;

– формированию государственного информационного ресурса;

– предоставлению в установленном порядке информации по вопросам лицензирования.

**Лицензия** – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа.

Основные понятия указанного закона: лицензируемый вид деятельности, лицензирующие органы, соискатель лицензии, лицензиат, лицензионные требования.

В соответствии с Федеральным законом "Об аккредитации в национальной системе аккредитации" **аккредитация** – подтверждение национальным органом по аккредитации соответствия юридического лица или индивидуального предпринимателя критериям аккредитации, являющееся официальным свидетельством компетентности юридического лица или индивидуального предпринимателя осуществлять деятельность в определенной области аккредитации.

Основные понятия указанного закона: выписка из реестра аккредитованных лиц (аттестат аккредитации), аттестация эксперта по аккредитации, заявитель, аккредитованное лицо, критерии аккредитации, область аккредитации.

**1. Виды и системы сертификации**

Международный стандарт ГОСТ ISO/IEC 17000–2012 "Оценка соответствия. Словарь и общие принципы" определяет три функции оценки соответствия:

1. Выбор, в рамках которого выполняется планирование и подготовка к получению доказательств, в том числе определяется методология оценки и отбирается собственно объект оценки;

2. Определение, в рамках чего проводится исследование характеристик объекта оценки и формируются соответствующие отчетные документы;

3. Итоговая проверка и подтверждение соответствия, в результате которых принимается и оформляется решение о соответствии или несоответствии объекта оценки заданным требованиям. Важной процедурой оценки соответствия является инспекционный контроль, представляющий собой систематическое наблюдение за деятельностью по оценке соответствия.

Кроме сертификации средств защиты информации можно встретить определения разного рода процедур оценки соответствия технических средств и систем защиты, а именно **испытания, аттестация, тестирование, аудит, анализ рисков**.

**Аттестация** – комплексная проверка защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации. Положительный результат аттестации оформляется в виде аттестата соответствия.

**Испытание** – вид деятельности или процедура по оценке соответствия, заключающаяся в экспериментальном определении количественных или качественных характеристик объекта испытаний как результата воздействия на него при его функционировании, моделировании или воздействий.

Результаты испытания оформляются в виде протоколов испытаний или технического отчёта.

*Аттестационные испытания* касаются объектов информатизации, включают выполнение стандартных детерминированных процедур, связанных, главным образом, с фиксацией состава, проверкой легитимности и корректности установки сертифицированных средств защиты информации.

*Сертификационные испытания* касаются средств защиты информации, проводятся испытательными лабораториями, включают длительные и трудоемкие процедуры проверки этих Средств, в том числе используя методы функционального и структурного тестирования и др.

**Тестирование** – это техническая операция, заключающаяся в определении одной или нескольких характеристик продукта, процесса или услуги по соответствующей процедуре. Под сертификацией понимается подтверждение соответствия третьей стороной, относящееся к продукции, процессам, системам или персоналу.

**Ключевые особенности сертификации**:

4. Сертификация проводится на соответствие заданным требованиям, а именно техническим регламентам, положениям стандартов, сводов правил, условиям договоров и другим требованиям, определенным в нормативных документах и соответствующей документации. Поэтому область сертификации и ее результат однозначно определены конкретными нормативными документами, а не требованиями и рекомендациями по повышению качеству или защищенности вообще.

5. В случае положительно результата процесс сертификации заканчивается выдачей официального письменно оформленного удостоверения – сертификата соответствия, а сертифицированная продукция подлежит маркировке знаком соответствия системы сертификации. В некоторых системах сертификации можно встретить еще одно официальное удостоверение – заключение, которое применяется для случаев, когда орган по сертификации затрудняется выдать общепринятый сертификат соответствия.

6. Сертификация является деятельностью третьей стороны, т.е. должна быть обеспечена независимость оценки соответствия, максимально исключающая любые формы аффилированности или сговора.

7. Сертификация может быть добровольной и обязательной. Сертификация средств защиты информации по требованиям безопасности информации является обязательной.

8. Так как в стране действует несколько систем сертификации, то эти системы определяют некоторые свои правила и процедуры проведения оценки соответствия, включая аккредитацию органов по сертификации и испытательных лабораторий, разумеется, в рамках российского законодательства и своей компетенции.

**Аудит** – систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания с целью установления степени выполнения заданных требований.

Отличия аудита от сертификации:

– нет жестких рамок в плане подтверждения соответствия в виде документа государственного образца (сертификата соответствия строго определенным требованиям);

– нет необходимости привлечения третьей стороны (независимой аккредитованной лаборатории);

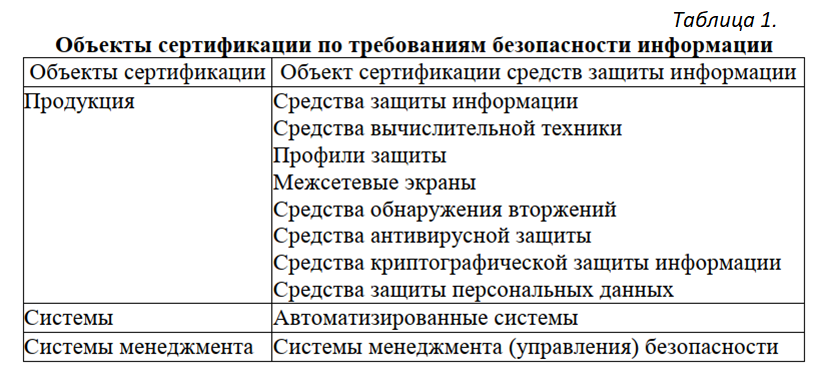
– критерии аудита могут быть более-гибкие, отвечающие реалиям дня.

Таким образом, сертификация средств защиты информации по требованиям безопасности информации представляет собой обязательное независимое подтверждение соответствия средств защиты информации (СЗИ) требованиям нормативных документов по защите информации с учетом правил федеральных органов (Минобороны, ФСБ, ФСТЭК) в рамках их компетенции.

Отметим, что федеральные органы по сертификации трактуют СЗИ в широком смысле, как средство защиты от угроз информационной безопасности и ее составных свойств: целостности, доступности, конфиденциальности и др. В этом смысле под понятие СЗИ при самой общей модели угроз подпадает любое изделие в защищенном исполнении, например, "безопасное" от программных закладок ПО.

**1.1. Объекты сертификации по требованиям безопасности информации**

В соответствии с "Положением о сертификации" СЗИ средствами защиты информации являются технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации. В таблице 1 приведены примеры объектов сертификации в области информационной безопасности, к которым определены требования в открытых нормативных документах.



На основании этого же положения указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. Система сертификации СЗИ представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам. Согласно указанному положению определены следующие системы сертификации СЗИ: ФСТЭК РФ, ФСБ РФ, Министерством обороны РФ, Службой внешней разведки РФ.

Указанные ведомства именуются как федеральные органы по сертификации. В каждой системе сертификации СЗИ разрабатываются и согласовываются с Межведомственной комиссией по защите государственной тайны положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Например, несмотря на то, что сертификация систем в ФСТЭК проводится в форме аттестации объектов информатизации, последняя реально (при защите конфиденциальной информации) таковой не является, т.к. не полностью соблюдается самый главный закон сертификации о третьей стороне.

Несмотря на то, что сформулированы требования к системам менеджмента информационной безопасности (серия ГОСТ 27000), они не нашли отражение в нормативно-методических документах обязательных систем сертификации. В жизни и в документах регуляторов можно встретить классы общепринятых СЗИ, таких как: средства контент анализа, средства контроля утечек, средства анализа защищенности, средства управления и мониторинга, средства доверенной загрузки, генераторы паролей, защищенные BIOS, средства безопасности программных приложений, средства безопасности виртуализации, средства безопасности облачных технологий, средства защиты в промышленных системах и системах высокой готовности и др., однако требования к ним либо пока отсутствуют, либо (в противоречие 2-му правилу Керкгоффса) не подлежат публичному информированию или обсуждению.

Согласно Доктрине информационной безопасности РФ сертификация СЗИ является важнейшим методом обеспечения безопасности страны, а значит, государственную важность приобретает совершенствование мер, направленных на повышение эффективности и достоверности результатов сертификации СЗИ. Именно поэтому процесс сертификации включает несколько уровней независимых проверок: экспертизу заявки в федеральном органе, проведение испытаний в аккредитованной испытательной лаборатории, проверку материалов испытаний в аккредитованном органе по сертификации и др. При этом обеспечивается независимость между участниками сертификации: аккредитованным органом по сертификации, аккредитованной испытательной лабораторией и другими заинтересованными сторонами.

**1.2. Правила и участники сертификации средств защиты информации.**

Согласно Постановлению Правительства РФ 1995 г. № 608, руководство системами сертификации возложено на федеральные органы по сертификации: Минобороны России, ФСБ России и ФСТЭК России.

В общегражданском плане регулирование рынка некриптографических СЗИ в стране возложено на ФСТЭК России, а рынка криптографических СЗИ – на ФСБ России.

Участниками сертификации являются:

1) федеральный орган по сертификации;

2) центральный орган системы сертификации (создаваемый при необходимости) – орган, возглавляющий систему сертификации однородной продукции;

3) органы по сертификации средств защиты информации - органы, проводящие сертификацию определенной продукции;

4) испытательные лаборатории – лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;

5) изготовители – продавцы, исполнители продукции.

Порядок проведения сертификации выглядит следующим образом.

1. Заявитель подает в федеральный орган заявку на проведение сертификационных испытаний.

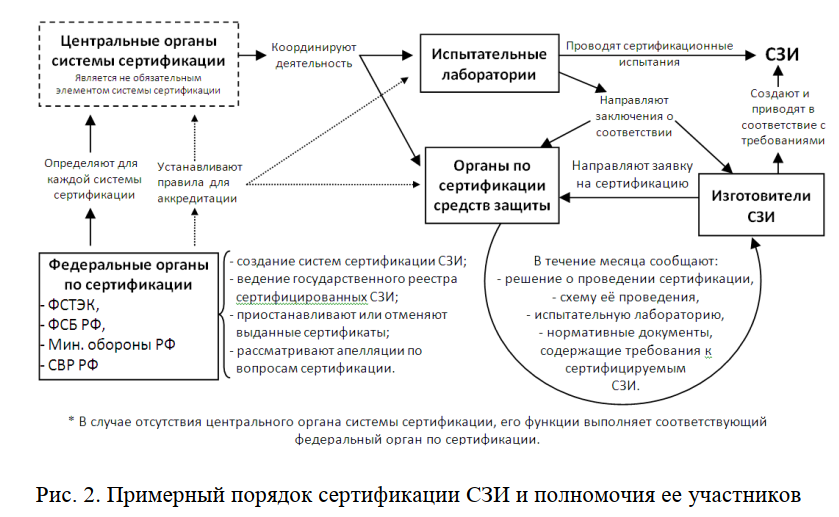
2. Федеральный орган определяет аккредитованную испытательную лабораторию и орган по сертификации, что фиксируется в решении на сертификацию.

3. Испытательная лаборатория проводитсертификационные испытания. Материалы испытаний (программа и методика, протоколы испытаний,

техническое заключение) передаются в орган по сертификации, который проводит их независимую экспертизу.

Взаимодействие участников системы сертификации ФСТЭК России представлены на рисунках 1, 2.





Федеральный орган по сертификации на основании положительного технического заключения органа по сертификации оформляет сертификат соответствия. В случае выявления каких-либо несоответствий федеральный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий и органов по сертификации.

**1.3. Схемы сертификации**

Основными схемами проведения сертификации средств защиты информации являются:

1. **Для** **единичных образцов** средств защиты информации – проведение испытаний этих образцов на соответствие требованиям по защите информации;

2. **Для серийного производства** средств защиты информации – проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный

контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе.

Максимальный срок действия сертификата не может превышать пяти лет.

Сертификационные испытания можно классифицировать по методу тестирования:

– функциональное тестирование продукта или системы по методу "черного ящика";

– структурное тестирование исходного кода ПО.

В первом случае при испытаниях используются:

– традиционные нормативные документы (например, руководящие документы Гостехкомисии России);

– документация (например, ТУ);

– задание по безопасности – документ, разрабатываемый в соответствии с метастандартом ГОСТ Р ИСО/МЭК 15408–1–...

Особенность структурного тестирования состоит в том, что оно проводится в форме статического и динамического анализа исходного кода программ и касается только вопросов внутренней безопасности продукта (контроля отсутствия недекларированных возможностей (НДВ)).

Документом, подтверждающим положительные результаты сертификационных испытаний, является сертификат соответствия, в котором указаны самые важные моменты: идентификационные характеристики, на соответствие каким документам проведены испытания, срок действия, документ (обычно технические условия (ТУ) или формуляр), в котором определены ограничения на использование СЗИ и зафиксированы контрольные суммы и др.

Перечень аккредитованных испытательных лабораторий ФСТЭК России и ФСБ России, аккредитованных органов по сертификации ФСТЭК, открытые реестры сертифицированных СЗИ, правовые акты и нормативно-

методические документы ФСТЭК и ФСБ можно посмотреть на веб-порталах указанных ведомств: **www.fstec.ru** и **clsz.fsb.ru**. Требования к сертификации определены федеральными законами, постановлениями Правительства, стандартами и кодексами, а требования к проверкам (сертификационным испытаниям, инженерным или тематическим исследованиям) определены в нормативных документах или в соответствующей документации.

**2. Нормативные, руководящие, нормативно-методические и методические документы ФСТЭК России и ФСБ России**

Законодательные и правовые требования определяют, когда сертификация необходима, а также ответственность за несоблюдение этих требований.

При определении обязательности сертификации СЗИ удобно провести классификацию защищаемого информационного ресурса и объектов информатизации. В качестве признаков классификации информационного ресурса выделяют два: принадлежность к государственному информационному ресурсу и уровень ограниченности доступа. Для государственного информационного ресурса требования устанавливает и контролирует сам собственник (государство). В других случаях могут быть неоднозначности. При идентификации уровня ограниченности доступа выделяют:

– государственную тайну;

– личную и семейную тайны (персональные данные);

– другие виды тайн, не отнесенные к государственной тайне и персональным данным;

– открытую общедоступную информацию.

В случае, когда говорят об информации ограниченного доступа, не отнесенной к государственной тайне, ее исторически часто называют информацией конфиденциального характера или просто конфиденциальной информацией.

Дополнительно могут быть определены требования к системам обработки информации, независимо от классификации обрабатываемой информации.

**2.1. Основания для обязательной сертификации средств защиты информации**

Основные случаи, когда сертификации СЗИ в нашей стране обязательна:

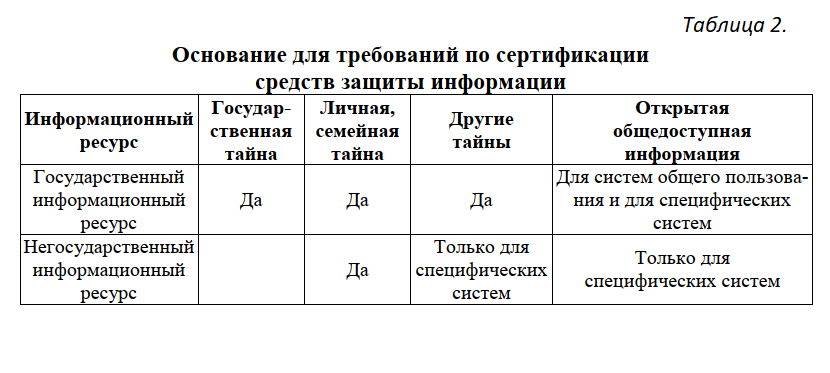
– защищаемая информация составляет сведения, отнесенные к государственной тайне;

– защищаемая информация ограниченного доступа, но не отнесенная к государственной тайне, при условии, что она относится к государственному информационному ресурсу;

– защищаемая информация относится к персональным данным и составляет личную и семейную тайну;

– к защите объектов информатизации (систем, комплексов) определены требования по оценке соответствия независимо от видов тайн.

Основания для требований по сертификации СЗИ представлены в таблице 2.



В случае защиты государственной тайны требования по обязательной сертификации СЗИ определены в Законе РФ "О государственной тайне" 1993 г. № 5485-I, Постановлении Правительства РФ 1995 г. № 608 [5] и в других документах.

Требования по сертификации средств защиты информации конфиденциального характера в государственных организациях определены в Постановлении Правительства РФ 2010 г. № 330 (п.6), а также в нормативных документах ФСБ России и ФСТЭК России.

Требования по сертификации средств защиты персональных данных прямо вытекают из Постановления Правительства РФ 2010 г. № 330 (п.6) и косвенно из Постановления Правительства РФ 2012 г. № 1119, а также

регламентируются нормативными документам ФСБ России и ФСТЭК России.

В остальных случаях необходимо руководствоваться нормативными требованиями к специфическим объектам. Примерами таких объектов являются:

– информационные системы критически важных объектов;

– автоматизированные системы управления технологическим процессом;

– системы управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства;

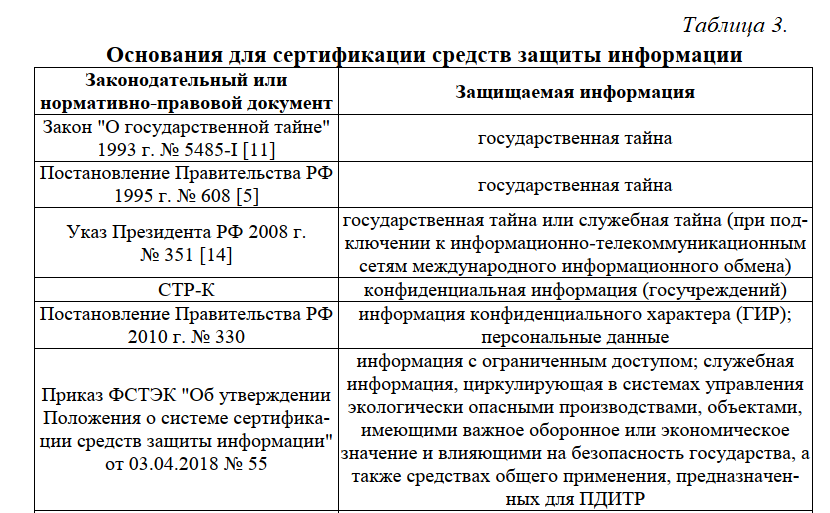
– федеральные государственные информационные системы общего пользования;

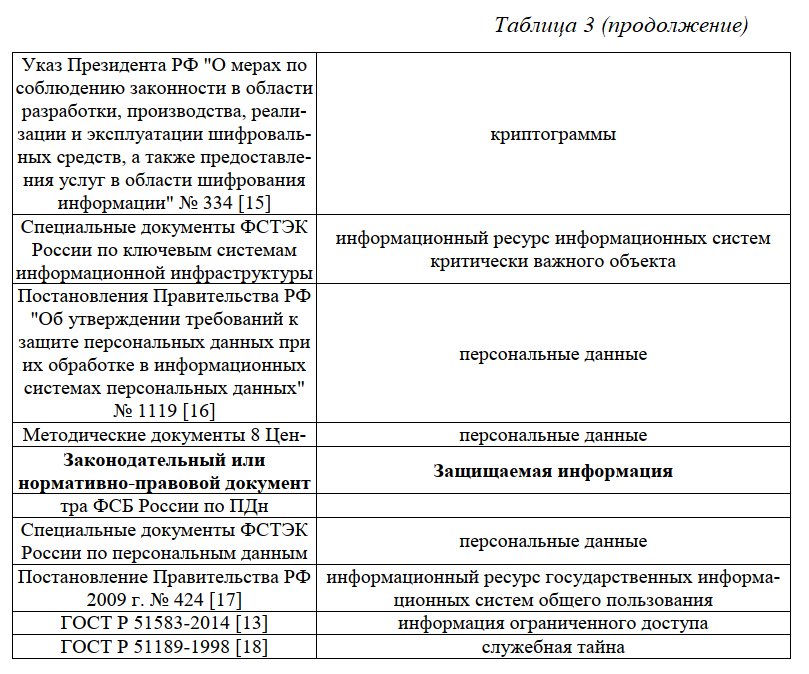
– автоматизированные системы систем вооружений;

– игровые автоматы и др.

С практической точки зрения обязательность сертификации СЗИ диктуется обычно двумя обстоятельствами. Первое связано с требованиями заказчика, который формулирует их к разработке, поставке, внедрению защищенной информационной системы. Например, в техническом задании или техническом проекте на ОКР (и дальнейшего авторского надзора или техподдержки) весьма красиво указать ГОСТ Р 51583–2014 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения". Согласно пункту 4.15 этого стандарта необходим сертификат соответствия.

Другой случай связан с необходимостью быть уверенным в защищенности объекта с формальной точки зрения, когда требуется заполучить какой-нибудь официальный документ о подтверждении соответствия информационной системы требованиям российского законодательства. В настоящее время в области информационной безопасности таким документом является аттестат соответствия. Никто не выпишет такой аттестат без сертифицированных СЗИ. Основания для сертификации СЗИ изложены в таблице 3.





Согласно Закону № 152-ФЗ "О персональных данных" лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. То же самое можно сказать и про использование несертифицированных СЗИ. Что касается административных нарушений в области защиты информации, то следует в первую очередь отметить Главу 13 действующего Кодекса Российской Федерации об административных правонарушениях (КоАП), в котором весьма интересны для изучения следующие статьи:

– статья 13.6. Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи;

– статья 13.12. Нарушение правил защиты информации;

– статья 13.13. Незаконная деятельность в области защиты информации.

Так, в статье 13.12 определены административные штрафы для случая использования несертифицированных СЗИ, включая конфискацию СЗИ, а при отягчающих обстоятельствах и высшую меру административного наказания - приостановление деятельности.

Уголовный кодекс РФ (УК РФ) вступает в силу, если внедрение и использование несертифицированных СЗИ квалифицируется как деяние, повлекшее некоторое преступление. Например, согласно статьи 274 УК РФ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации может ограничить свободу на пять лет. Вопросы нарушения правил и условий, халатности, утраты, разглашения тайн при автоматизированной обработке в той или иной степени отражены в 19, 22, 24, 26-33 главах УК РФ.

**Отдельно следует назвать статью 171 (незаконное предпринимательство)**, касающуюся деятельности с нарушением обязательных лицензионных требований и условий при разработке, внедрении и сертификации СЗИ.

Надо понимать, что ответственность за возникшие проблемы в области защиты информации, кроме органов по сертификации и испытательных лабораторий, возлагается также на владельца объекта информатизации, уполномоченного владельцем (по договору) лицо и разработчика.

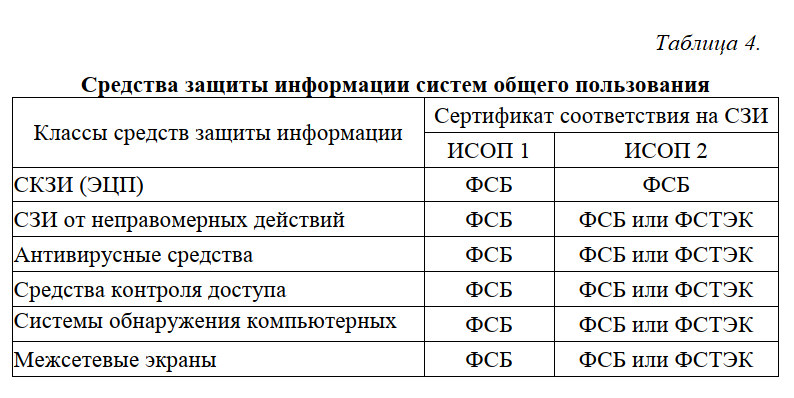
**2.2. Требования к защите информационных систем общего пользования**

Несмотря на то, что информационный ресурс федеральных информационных систем общего пользования (порталов, оказывающих конституционные услуги) открытый и общедоступный, он подлежит защите сертифицированными средствами. Например, Постановлением Правительства РФ 2009 г. № 424 "Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям« определено, что при подключении таких систем к информационно-телекоммуникационным сетям, доступ к которым не ограничен (например, метасеть Интернет), необходимо использовать СЗИ, прошедшие оценку соответствия. Дополнительные требования к СЗИ определены совместным Приказом ФСБ России и ФСТЭК России 2010 г. №416/№484 "Об утверждении требований о защите информации, содержащихся в информационных системах общего пользования" [20] в зависимости от класса системы. Приказ обозначил два класса информационных систем общего пользования (ИСОП);

– системы 1-го класса, к которым относятся ИСОП Правительства РФ и другие ИСОП, нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности страны;

– системы 2-го класса, к которым относятся остальные все ИСОП.

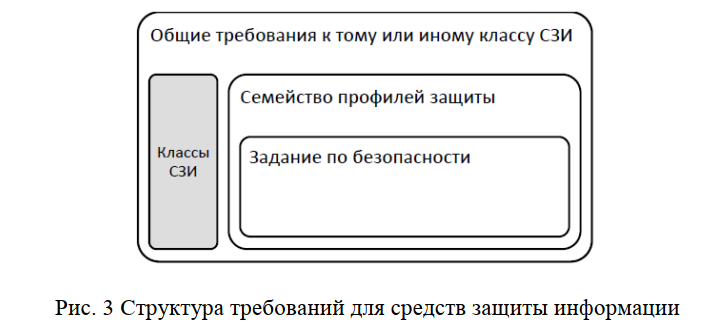
Решение об отнесении к классу ИСОП определяется руководителем соответствующего федерального органа исполнительной власти. Особенностью объединенного Приказа является введение требований по использованию сертифицированных классов СЗИ, представленных в таблице 4.



Конкретные требования к классам защищенности средств защиты общедоступной информации не определены в открытой печати, за исключением систем обнаружения вторжений и антивирусных средств для ИСОП 2. Согласно нормативным документам ФСТЭК России названные средства должны соответствовать ОУД 2+(усиленный). В остальных случаях необходимо ориентироваться на модель нарушителя, модель угроз и технологии обрабатываемой информации.

**2.3. Современные нормативные документы ФСТЭК России**

На сегодняшний день при проведении сертификационных испытаний СЗИ по требованиям безопасности информации в абсолютном большинстве случаев используются традиционные руководящие документы Гостехкомиссии России. Несмотря на некоторое моральное устаревание данных документов, применение "Общих критериев" при проведении сертификационных испытаний до последнего времени было весьма ограниченно и носило скорее экспериментальный характер. В то же время перспективы развития оценочных стандартов в данной области сейчас связаны, прежде всего, с "Общими критериями". В настоящее время в ФСТЭК России разработаны документы, касающиеся требований к системам обнаружения вторжений и антивирусных средств. Ожидается, что в ближайшее время на базе "Общих критериев" будут разработаны требования к средствам доверенной загрузки, средствам двухфакторной аутентификации, средствам контроля съемных носителей информации, средствам предотвращения утечек информации и др. В общем случае, стандарты нового поколения будут иметь структуру, представленную на рисунке 3.



Для каждого из основных классов средств защиты информации будет разработан документ, классифицирующий данный вид средств защиты и определяющий требования к соответствующему семейству профилей защиты. В свою очередь, профили защиты должны служить основанием для разработки заданий по безопасности, на соответствие которым и будет сертифицироваться конечный продукт.

В настоящий момент ФСТЭК России сформулировал требования к системам обнаружения вторжений (СОВ) и системам антивирусной защиты (САВЗ). Документы вступили в силу в 2012 г., но имеют пометку "для служебного пользования". Профили защиты СОВ и САВЗ, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, являются общедоступными и в настоящее время размещены на официальном сайте ФСТЭК России.

**Лекция 7-8. Законодательство РФ в области информационной безопасности**

1. Основы законодательства
2. Стратегические документы
3. Системообразующие документы
4. Государственные регуляторы
5. Техническое регулирование
6. Техническое регулирование. Сертификация средств защиты информации
7. Техническое регулирование. Аттестация объектов информатизации
8. Лицензирование деятельности в области ИБ
9. ИБ и персонал
10. Судебные тяжбы, компьютерная криминалистика
11. Ответственность за нарушения в области ИБ
12. Руководящие документы ФСТЭК России
13. Криптография
14. Электронная подпись
15. Государственная тайна
16. Служебная тайна
17. Коммерческая тайна
18. Банковская тайна
19. Инсайдерская информация
20. Защита связи
21. Государственные и муниципальные информационные системы (ГИС и МИС)
22. Государственные и муниципальные информационные системы. СМЭВ
23. Государственные и муниципальные информационные системы. Обеспечение безопасности
24. Государственные и муниципальные информационные системы. Открытые данные
25. Государственные и муниципальные информационные системы. Московская область
26. Государственные и муниципальные информационные системы. Здравоохранения и медицина
27. Подключение к Интернет государственных систем
28. Критическая информационная инфраструктура (КИИ)
29. Критическая информационная инфраструктура. Связь
30. Топливно-энергетический комплекс (ТЭК)
31. Транспорт
32. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
33. Персональные данные (ПДн)
34. Персональные данные. Обеспечение безопасности
35. Персональные данные. Блокировка нарушителей
36. Персональные данные. Банковская специфика
37. Персональные данные. Единая биометрическая система (ЕБС)
38. Персональные данные. Особые случаи обработки ПДн
39. Персональные данные. Сроки хранения
40. Персональные данные. Международные требования
41. Персональные данные. Примеры внутренних документов
42. Национальная платежная система
43. Банковская безопасность. Нормативно-правовые акты Банка России
44. Банковская безопасность. Стандарты Банка России
45. Банковская безопасность. ГОСТы по безопасности
46. Банковская безопасность. Криптография
47. Некредитные финансовые организации (НФО)
48. Международные требования по безопасности платежных карт
49. Здравоохранение
50. Образование
51. Государственные корпорации
52. Идентификация и аутентификация
53. Служба информационной безопасности организации

**Государственные регуляторы**

1. ФСТЭК России
2. ФСБ России
3. Министерство цифрового развития, связи и массовых коммуникаций РФ(Минкомсвязь)
4. Роскомнадзор
5. Банк России
6. Министерство обороны РФ и Генеральный штаб ВС РФ
7. Министерство юстиции РФ
8. Министерство иностранных дел РФ
9. Межведомственная комиссия СБ РФ по вопросам обеспечения технологического суверенитета
10. Межведомственная комиссия СБ РФ по информационной безопасности по должностям

**Техническое регулирование**

1. N 184-ФЗ от 27.12.2002 «О техническом регулировании»

Комментарий. Здесь под техническим регулированием подразумевается: стандартизация (определение необходимости использования национальных или международных стандартов), определение процедур оценки соответствия средств защиты информации (например, обязательная сертификация), определение мероприятий по аттестации объектов информатизации по требованиям безопасности информации, особенности проведения измерений.

1. N 102-ФЗ от 26.06.2008 «Об обеспечении единства измерений»
2. N 162-ФЗ от 29.06.2015 «О стандартизации в Российской Федерации»
3. ППРФ от 30.12.2016 N 1567 «О порядке стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих ГТ или относимых к охраняемой в соответствии с законодательством РФ иной инф-и ограниченного доступа, продукции, сведения о которой составляют ГТ, а также процессов и иных объектов стандартизации, связанных с такой продукцией»
4. Пр. Минкомсвязи России от 22.09.2020 N 486 «Об утверждении классификатора программ для ЭВМ и БД» (Зарег.в Минюсте России 29.10.2020 N 60646)

Комментарий. Документ содержит классификатор средств защиты информации.

**Техническое регулирование. Сертификация средств защиты информации**

1. N 218-ФЗ от 30.12.2004 «О кредитных историях»

Комментарий. Закон устанавливает обязанность использования бюро кредитных историй сертифицированных средств защиты информации.

1. ПП РФ от 26.06.1995 N 608 «О сертификации средств защиты информации»
2. ПП РФ от 01.12.2009 N 982 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии»

Комментарий. п.4 Постановления гласит, что оно не распространяется на средства защиты информации.

1. ПП РФ от 21.04.2010 N 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих ГТ или относимых к охраняемой в соответствии с зак-ом РФ иной инф-и ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют ГТ, предназначенной для эксп-и в загранучреждениях РФ, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксп-и, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о серт.СЗИ» (вместе с «Положением об особенностях оценки соответствия продукции (работ, услуг,) используемой в целях защиты сведений, …»)
2. Пр. ФСТЭК России от 10.04.2015 N 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих ГТ или относимых к охраняемой в соответствии с зак-ом РФ иной инф-и ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности» (Зарег.в МЮ 20.05.2015 N 37342).
3. Пр. ФСТЭК России от 03.04.2018 N 55 «Об утверждении Положения о системе сертификации средств защиты информации» (Зарег.в МЮ 11.05.2018 N 51063).

**Техническое регулирование. Аттестация объектов информатизации**

Комментарий. Необходимость обязательной аттестации объектов информатизации по требованиям безопасности информации содержится также и в других документах, например, в Пр.е ФСТЭК России от 11.02.2013 N 17 и др.

1. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994)
2. «Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации» (утв. Пр.ом Гостехкомиссии от 05.01.1996 N 3)
3. Пр. ФСТЭК России от 29.04.2021 N 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»
4. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от 02.09.2021 г. N 240/24/4303 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»
5. Информационное сообщение Минцифры РФ от 03.06.2022 «Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры»
6. Информационное сообщение ФСТЭК России от 11.04.2022 г. N 240/24/1950 «О порядке представления документов по аттестации объектов информатизации, обрабатывающих информацию ограниченного доступа, не составляющую государственную тайну»

**Лицензирование деятельности в области информационной безопасности**

1. N 99-ФЗ от 04.05.2011 «О лицензировании отдельных видов деятельности»

Комментарий. Лицензирование деятельности, связанной с защитой или обработкой государственной тайны, осуществляется в соответствии с законом «О государственной тайне» и выпущенными на его основе документами.

1. ПП РФ от 01.06.1996 N 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных для негласного получения информации, и перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности»
2. ПП РФ от 21.11.2011 N 957 «Об организации лицензирования отдельных видов деятельности»
3. ПП РФ от 03.02.2012 N 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»)
4. ПП РФ от 03.03.2012 N 171 «О лицензировании деят.по разработке и производству средств защиты конф.инф-и» (вместе с «Положением о лицензировании деят. по разработке и производству средств защиты конф.инф-и»)
5. ПП РФ от 12.04.2012 N 287 «Об утверждении Положения о лицензировании деят. по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения инф-и»
6. ПП РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, инф.систем и телеком.систем, защищенных с исп-м шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифр. (крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крип.) средств (за исключением случая, если техническое обслуживание шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крипт.) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
7. ПП РФ от 16.04.2012 N 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
8. Пр. ФСБ России от 30.08.2012 N 440 «Об утверждении Административного регламента ФСБ РФ по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крипт.) средств, выполнению работ, оказанию услуг в области шифрования инф-и, техническому обслуживанию шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крипт.) средств (за исключением случая, если техническое обслуживание шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шиф.(крипт.) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
9. Пр. ФСБ России от 23.03.2016 N 182 «Об утверждении Адм.регл. ФСБ РФ по исполнению государственной функции по осуществлению лицензионного контроля деятельности по разработке, производству, распространению шифр.(крипт.) средств, инф.систем и телеком. систем, защищенных с использованием шифр.(крипт.) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крипт.) средств (за исключением случая, если техническое обслуживание шифр.(крипт.) средств, инф.систем и телеком.систем, защищенных с использованием шифр.(крипт.) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» (Зарег.в МЮ 18.04.2016 N 41821)
10. Пр. ФСТЭК России от 17.07.2017 N 133 «Об утверждении Адм. регламента ФСТЭК по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации» (Зарег.в МЮ 11.08.2017 N 47757)

12. ПЕРЕЧЕНЬ технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным ПП РФ от 3.02.2012 г. N 79 [ФСТЭК России]

Комментарий. В документе содержится исчерпывающий перечень основных руководящих документов ФСТЭК России.

13. ПЕРЕЧЕНЬ контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным ПП РФ от 3.02.2012 г. N 79 [ФСТЭК России]

14. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от 26 марта 2015 г. N 240/13/1139 «О типичных ошибках, допускаемых соискателями лицензий при подготовке и представлении документов для получения лицензий на деятельность по технической защите конфиденциальной информации и на деятельность по разработке и производству средств защиты конфиденциальной информации»

15. Пр. ФСБ России от 31.01.2022 N 35 «Об утверждении форм документов, используемых Федеральной службой безопасности РФ в процессе лицензирования в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ „О лицензировании отдельных видов деятельности“ (Зарег. в МЮ 16.02.2022 N 67300)

16. Пр. ФСТЭК России от 28.12.2021 N 206 „Об утверждении формы оценочного листа, в соответствии с которым ФСТЭК России проводит оценку соответствия соискателя лицензии или лицензиата лицензионным требованиям при осуществлении деятельности по технической защите конфиденциальной информации“ (Зарег. в МЮ 28.02.2022 N 67507)

17. Пр. ФСТЭК России от 28.12.2021 N 207 „Об утверждении формы оценочного листа, в соответствии с которым ФСТЭК России проводит оценку соответствия соискателя лицензии или лицензиата лицензионным требованиям при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации“ (Зарег.в МЮ 28.02.2022 N 67506)

**Руководящие документы ФСТЭК России**

Комментарий. С полным перечнем руководящих документов ФСТЭК России можно ознакомиться в «Перечне технической документации…, утвержденным ПП РФ от 3.02.2012 г. № 79 (новая редакция)».

1. Инф. Сообщ.ФСТЭК России от 29.03.2019 N 240/24/1525 «О требованиях по безопасности инф-и, устанавливающих уровни доверия к средствам технической ЗИ и средствам обеспечения безопасности инф.технологий»
2. Инф.сообщ.ФСТЭК России от 20.01.2020 N 240/24/250 «О применении сертифицированных операционных Microsoft Windows 7 и Microsoft Windows Server 2008 r2 в связи с прекращением их технической поддержки»
3. Письмо ФСТЭК России от 20.03.2020 N 240/84/389 «Рекомендации по обеспечению безопасности объектов КИИ при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов КИИ»
4. «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021)
5. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» (утв. Пр.ом ФСТЭК России от 02.06.2020 N 76)

**Криптография**

1. Указ Президента РФ от 03.04.1995 N 334 «О мерах по соблюдению законности в области разработки, производства, реализации и экспл. шифровальных средств, а также предоставления услуг в области шифр-ия инф-и»
2. Поручение Президента от 16 июля 2016 года № Пр-1380 «Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование рос. крипт. алгоритмов и средств шифр-ия»
3. ПП РФ от 30.06.2020 № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в ГИС»
4. Пр. ФАПСИ от 13.06.2001 N 152 «Об утв-ии Инструкции об орг-ии и обесп-ии без-ти хранения, обработки и передачи по каналам связи с исп-ем средств крипт. ЗИ с огр.доступом, не содержащей сведений, составляющих ГТ» (Зарег.в Минюсте РФ 06.08.2001 N 2848)
5. Пр. ФСБ РФ от 09.02.2005 N 66 «Об утв. Положения о разработке, производстве, реализации и экспл. шифровальных (крипт.) СЗИ (Положение ПКЗ-2005)» (Зарег.в Минюсте РФ 03.03.2005 N 6382)
6. Решение Коллегии Евразийской экон. комиссии от 06.11.2014 N 199 «Об Инстр.об оформлении заявл-я на выдачу лицензии на экспорт и (или) импорт отд.видов товаров и об оформлении такой лицензии и Инструкции об оформлении разр-я на экспорт и (или) импорт отд. видов товаров»

Комментарий. Данный документ определяет порядок оформления лицензий (в случае необходимости) на ввоз/вывоз криптографических средств через границу Таможенного союза ЕАЭС.

1. Решение Коллегии Евразийской экон. комиссии от 21.04.2015 N 30 «О мерах нетарифного регулирования» (вместе с «Положением о ввозе на таможенную территорию Евразийского экон.союза и вывозе с таможенной территории ЕЭС органов и тканей человека, крови и ее компонентов, образцов биол. материалов человека», «Положением о вывозе с тамож. территории ЕЭС минерального сырья», «Положением о вывозе с тамож. территории ЕЭС диких живых животных, отдельных дикорастущих растений и дикораст. лекарственного сырья», «Положением о вывозе с тамож. территории ЕЭС редких и находящихся под угрозой исчезновения видов диких живых животных и дикораст. растений, включенных в красные книги государств — членов ЕЭС», «Положением о ввозе на тамож. терр-ю ЕЭС и вывозе с тамож. терр-и ЕЭС опасных отходов», «Положением о вывозе с тамож. территории ЕЭС культурных ценностей, документов национальных архивных фондов и оригиналов архивных документов», «Положением о ввозе на тамож. территорию ЕЭС и вывозе с тамож.территории ЕЭС *шифровальных (крипт.) средств*», «Положением о ввозе на тамож. территорию ЕЭС и вывозе с тамож. территории ЕЭС наркотических средств, психотропных веществ и их прекурсоров»)
2. ИЗВЕЩЕНИЕ ФСБ России от 18.07.2016 по вопросу использования несертиф. средств кодирования (шифрования) при передаче сообщений в инф.-телеком. сети «Интернет»
3. Пр. ФСБ России 19.07.2016 года N 432 «Об утверждении Порядка представления организаторами распространения инф-ии в инф.-телеком. сети „Интернет“ в ФСБ РФ информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей инф.-телеком. сети „Интернет“»
4. Извещение ФСБ России от 01.07.2019 «О порядке использования алгоритма блочного шифрования ГОСТ 28147-89»
5. Извещение ФСБ России от 01.07.2019 «Об использовании атрибута имени «localityName» поля «subject» в структуре квалифицированного сертификата ключа проверки электронной подписи»
6. Требования к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну (выписка от 23.09.2019)
7. ППРФ от 09.05.2022 N 834 «Об установлении особенностей ввоза в Российскую Федерацию шифровальных (криптографических) средств и товаров, их содержащих»

**Электронная подпись**

1. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
2. ППРФ от 09.02.2012 N 111 «Об ЭП, используемой органами исп. власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств ЭП
3. ППРФ от 25.01.2013 N 33 „Об исп-ии простой ЭП при оказании государственных и муниципальных услуг“ (вместе с „Правилами использования простой ЭП при оказании гос. и муниц. услуг“)
4. ППРФ от 07.07.2017 N 807 „Об утверждении Правил использования усиленных квалифицированных   
   ЭП при ведении Единого государственного реестра записей актов гражданского состояния и переводе в электронную форму книг государственной регистрации актов гражданского состояния (актовых книг)“
5. ППРФ от 28.12.2020 N 2309 „Об утверждении требований к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им кв.серт-ах с использованием единого портала гос-х и мун. услуг“
6. ППРФ от 31.12.2020 N 2440 „Об утверждении Правил использования усиленной квалифицированной электронной подписи при формировании и ведении единого фед. инф. регистра, содержащего сведения о населении РФ“
7. ППРФ от 15.10.2021 N 1754 „Об утверждении требований к проверке простой ЭП, которой в соответствии с частями 5 и 23 статьи 14.1 фед. закона “Об информации, информационных технологиях и о защите информации» подписаны согласия на обработку ПДн и БПДн , при хранении указанных согласий"
8. ППРФ от 21.02.2022 N 222 «Об утв-ии Правил представления заинт. лицам документа о полномочиях физического лица в случае, предусмотренном частью 2 статьи 17.1 ФЗ „Об ЭП“
9. ППРФ от 21.02.2022 N 223 „Об утв-ии орг.-технических требований к порядку хранения, использования и отмены указанных в статьях 17.2 и 17.3 ФЗ “Об ЭП» доверенностей"
10. ППРФ от 21.02.2022 N 224 «Об утверждении треб-й к норм. правовым актам фед. органов исп. власти, устанавливающим порядок представления доверенности в предусмотренном п.2 части 1 статьи 17.2 ФЗ „Об ЭП“ случае, и требований к порядку представления доверенности в предусмотренном п.2 статьи 17.3 ФЗ „Об ЭП“ случае»
11. Пр. ФСБ РФ от 27.12.2011 N 795 «Об утверждении Требований к форме квалиф.сертификата ключа проверки ЭП»
12. Пр. ФСБ РФ от 27.12.2011 N 796 «Об утверждении Требований к средствам ЭП и Треб-ий к средствам УЦ» (Зарег.в Минюсте РФ 09.02.2012 N 23191)
13. Пр. Минсвязи и массовых коммуникаций РФ от 30.11.2015 N 486 «Об утв. адм. регламентов предоставления Минсвязи и масс.комм-ий РФ гос. услуги по аккредитации УЦ и исполнения Минсвязи и МК РФ гос. функции по осуществлению гос. контроля и надзора за соблюдением аккредитованными УЦ требований, которые установлены ФЗ „Об ЭП“ и на соответствие которым эти УЦ были аккредитованы»
14. Пр. Минкомсвязи России от 22.08.2017 N 436 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров» (Зарег.в МЮ 22.09.2017 N 48283)
15. Пр. Минкомсвязи России от 13.08.2018 N 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей» (Зарег.в МЮ 17.12.2018 N 53026)
16. Пр. Минкомсвязи России от 14.09.2020 N 472 «Об утверждении Формата ЭП, обязательного для реализации всеми средствами ЭП» (Зарег. в Минюсте России 29.10.2020 N 60631)
17. Пр. ФНС России от 12.10.2020 N ЕД-7-14/743@ «Об утверждении Порядка взаимодействия с регистрирующим органом при направлении документов, необходимых для гос. регистрации юр. лиц и ИП, в форме электронных документов, а также требований к формированию таких электронных документов» (Зарег. в Минюсте России 29.10.2020 N 60640)
18. Пр. Минцифры России от 26.11.2020 N 624 «Об утверждении перечня угроз безопасности, актуальных при идент. заявителя — физ. лица в аккредитованном УЦ, выдаче квал. серт-а без его личного присутствия с применением инф.технологий путем предоставления сведений из Есистемы идент. и аутент-ии и Еинф. системы ПД, обеспечивающей обработку, сбор и хранение БПД, их проверку и передачу инф-ии о степени их соответствия предоставленным биометрическим ПД гражданина РФ, а также хранении и использовании ключа ЭП в аккредитованном УЦ» (Зарег.в МЮ 22.12.2020 N 61689)
19. Пр. ФНС России от 30.12.2020 N ВД-7-24/982@ «Об утверждении Порядка реализации ФНС функций аккредитованного УЦ и исполнения его обязанностей» (Зарег. в Минюсте России 14.05.2021 N 63416)
20. Пр. ФСБ России от 20.04.2021 N 154 «Об утверждении Правил подтверждения владения ключом ЭП» (Зарег.в МЮ 31.05.2021 N 63700)
21. Пр. ФСБ России от 01.05.2021 N 171 «Об утверждении организационно-технических требований в области ИБ к доверенным лицам УЦ фед. органа исп. власти, уполномоченного на осуществление гос. регистрации юридических лиц» (Зарег. в Минюсте России 01.06.2021 N 63741)
22. «Метод. рекомендации по порядку обмена электронными документами между хозяйствующими субъектами или физическими лицами» (утв. ФНС России)
23. Пр. Казначейства России от 15.06.2021 N 21н «Об утверждении Порядка реализации Федеральным казначейством функций аккредитованного УЦ и исполнения его обязанностей» (Зарег. в Минюсте России 09.08.2021 N 64574)
24. <Письмо> Минцифры России от 10.08.2021 N ОП-П15-085-33604 <О разъяснении применения положений ФЗ N 63 от 06.04.2011>
25. Пр. Минцифры России от 27.08.2021 N 896 «Об утверждении требований к деловой репутации единоличного исп. органа или членов коллегиального исп. органа орг-ии, владеющей инф. системой, обеспечивающей идент-ю и (или) аутент-ю с исп-ем биом.ПД физ. лиц, и (или) оказывающей услуги по идент-и и (или) аутент-и с исп-ем биом.ПД физ. лиц» (Зарег.в Минюсте России 17.09.2021 N 65045)
26. Пр. Минцифры России от 18.08.2021 N 856 «О порядке формирования, актуализации классификатора полномочий и обеспечения доступа к нему» (Зарег. в Минюсте России 08.10.2021 N 65350)
27. Пр. Минцифры России от 18.08.2021 N 857 «Об утверждении единых требований к формам доверенностей, необходимых для использования квал. ЭП» (Зарег. в Минюсте России 08.10.2021 N 65353)
28. Пр. Минцифры России от 18.08.2021 N 858 «Об утверждении единых требований к машиночитаемым формам документов о полномочиях» (Зарег. в Минюсте России 08.10.2021 N 65351)
29. Пр. Минцифры России от 02.11.2021 N 1134 «Об утв. Порядка передачи реестров выданных аккредитованными УЦ квал. сертификатов ключей проверки ЭП и иной инф-и в фед. орган исп. власти, уполномоченный в сфере использования ЭП, в случае прекращения деятельности аккредитованного УЦ» (Зарег. в Минюсте России 30.11.2021 N 66141)
30. Пр. Минцифры России от 08.11.2021 N 1138 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными УЦ квалифицированных сертификатов ключей проверки ЭП, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации» (Зарег.в МЮ 30.11.2021 N 66117)
31. Письмо Федеральной налоговой службы от 3 июня 2022 г. N ЕА-3-26/5811@ О применении доверенности, совершённой в электронной форме и подписанной усиленной квалифицированной ЭП доверителя

**Государственная тайна**

1. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»
2. N 61-ФЗ «Об обороне» от 31.05.1996 Комментарий. Раздел 3.1 настоящего закона вводит понятие «Служебная тайна в области обороны».
3. ПП РФ от 15.04.1995 N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих ГТ, созданием СЗИ, а также с осуществлением мероприятий и (или) оказанием услуг по защите ГТ»
4. ПП РФ от 04.09.1995 N 870 «Об утверждении Правил отнесения сведений, составляющих ГТ, к различным степеням секретности»
5. Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к ГТ»
6. ПП РФ от 06.02.2010 N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к ГТ»
7. Пр. ФСБ России от 28.09.2021 N 379 «Об утверждении Перечня сведений в области военной, военно-технической деятельности РФ, которые при их получении иностранным государством, его государственными органами, международной или иностранной орг-ей, иностранными гражданами или лицами без гражданства могут быть использованы против безопасности РФ».

**Служебная тайна**

1. ПП РФ от 03.11.1994 N 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исп.власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»
2. Пр. Министра обороны РФ от 17.01.2022 N 22 «Об утверждении Перечня сведений ВС РФ, подлежащих отнесению к служебной тайне в области обороны» (Зарег. в Минюсте России 28.02.2022 N 67528)

**Коммерческая тайна**

Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

**Банковская тайна**

Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности»

Комментарий. Понятие банковской тайны также определено в ГК РФ.

**Инсайдерская информация**

1. N 224-ФЗ от 27.07.2010 «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
2. Указание Банка России от 11.09.2014 N 3379-У «О перечне инсайдерской информации лиц, указанных в пунктах 1 — 4, 11 и 12 статьи 4 фед. закона „О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации“ (Зарег.в МЮ 15.10.2014 N 34325)

**Защита связи**

1. Федеральный закон от 17.07.1999 N 176-ФЗ „О почтовой связи“
2. Федеральный закон от 07.07.2003 N 126-ФЗ „О связи“
3. ПП РФ от 25.06.2009 N 532 „Об утв. перечня средств связи, подлежащих обязательной сертификации“
4. ПП РФ от 27.08.2005 N 538 „Об утв. Правил взаимодействия операторов связи с уполн. гос. органами, осуществляющими опер.-роз. деят-ть“
5. ПП РФ от 14.11.2014 N 1194 „О м/н-правовой защите присвоения (назначения) радиочастот или р/ч каналов и порядке исп-ия на терр-и РФ спутник.сетей связи, находящихся под юрисд. ин. гос-тв, а также о внесении изменений в нек.акты Правительства РФ“ (вместе с „Правилами проведения в РФ работ по м/н-правовой защите присвоения (назн-я) радиочастот или р/ч каналов“, „Правилами исп-ия на терр-и РФ спутн. сетей связи, наход-ся под юрисд. ин. гос-в“)
6. ПП РФ от 12.04.2018 N 445 „Об утв. Правил хранения операторами связи текстовых сообщений польз-ей услугами связи, голосовой инф-ии, изображений, звуков, видео- и иных сообщений пользователей услугами связи“
7. ПП РФ от 12.10.2019 N 1316 „Об утв. Положения о пров-ии учений по обеспечению устойч., безоп. и целостного функционирования на терр. РФ инф.-телеком. сети “Интернет» и сети связи общего пользования"
8. Пр. Мининформсвязи РФ от 09.01.2008 N 1 «Об утверждении треб-ий по защите сетей связи от НСД к ним и передаваемой посредством их информации» (Зарег. в Минюсте РФ 23.01.2008 N 10993)
9. Пр. Минкомсвязи России от 27.06.2011 N 160 «Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VI. Правила применения узлов связи с территориально распределенной архитектурой стандартов UMTS и/или GSM 900/1800» (Зарег.в МЮ 20.07.2011 N 21423)
10. Пр. Минцифры России от 02.03.2022 N 156 «Об утверждении Порядка защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения вызова экстренных оперативных служб по единому номеру „112“ (Зарег.в МЮ 01.06.2022 N 68676)

**Гос. и муниц. информационные системы (ГИС и МИС)**

Комментарий. Основным федеральным законом про ГИС и МИС является N 149-ФЗ от 27.07.2006.

1. N 59-ФЗ от 02.05.2006 „О порядке рассмотрения обращ-й граждан РФ“

Комментарий. Требования данного закона должны учитываться при разработке ГИС, используемых для взаимодействия с гражданами.

1. N 262-ФЗ от 22.12.2008 „Об обеспечении доступа к инф-ии о деят. судов в РФ“

Комментарий. Описывает особенности использования ИС в судах

1. N 8-ФЗ от 09.02.2009 „Об обеспечении доступа к инф-ии о деят-ти гос. органов и орг-в местного самоуправления“

Комментарий. Описывает особенности использования ИС в гос.органах, в том числе обязанность публиковать перечни используемых ИС.

1. Закон РФ от 11.02.1993 года N 4462-1 „Основы законодательства РФ о нотариате“

Комментарий. Глава VII.1. посвящена Еинф. системе нотариата.

1. N 20-ФЗ „О Гос-ой автомат. системе РФ «Выборы» от 10.01.2003
2. Пр. Управления делами Президента РФ от 03.10.2017 N 402 «Об утв. Порядка организации работы по обесп-ю доступа к инф-ии о деят. Управ.делами Президента РФ» (Зарег. в Минюсте России 31.10.2017 N 48737)
3. ПП РФ от 18.05.2009 N 424 «Об особенностях подключения федер. ГИС к инф.-телеком. сетям»
4. ПП РФ от 24.11.2009 N 953 «Об обесп-и доступа к инф-и о деят. Правительства РФ и фед. органов исп. власти» (вместе с «Треб-ми к технол., программным и лингв-им средствам обеспечения пользования оф. сайтом Прав.РФ в сети Интернет»)
5. ПП РФ от 08.09.2010 N 697 «О Единой системе межвед. электр. взаимодействия» (вместе с «Положением...»)
6. ПП РФ от 08.06.2011 N 451 «Об инфраструктуре, обесп-ей инф.-технол.взаимодействие инф.систем, исп-ых для предост. гос. и муниц. услуг и исполн-я гос.и мун.функций в эл. форме» (вместе с «Положением …»)
7. ПП РФ от 28.11.2011 N 977 «О фед. гос. инф. системе „Единая система идент-и и аутент-и в инфраструктуре, обесп-ей инф.-технол. взаимодействие инф.систем, исп-ых для предоставления гос.и мун.услуг в эл. форме“ (вместе с „Требованиями …»)
8. ПП РФ от 26.06.2012 N 644 «О фед.гос.инф. системе учета инф. систем, создаваемых и приобретаемых за счет средств фед. бюджета и бюджетов гос. внебюдж. фондов» (вместе с «Положением о ФГИС учета ИС…»)
9. ПП РФ от 10.07.2013 N 584 «Об исп-и ФГИС „Единая система идент. и аутент. в инфраструктуре, обеспечивающей инф.-технол. взаимодействие ИС, используемых для предоставления гос.и мун.услуг в эл.форме“ (вместе с „Правилами…»)
10. ПП РФ от 31.07.2014 N 747 «О перечне личных, семейных и домашних нужд, удовлетворение которых не влечет исполнения обязанностей, предусмотренных частями 2 — 4 статьи 10.1 фед. закона „Об информации, информационных технологиях и о защите информации“
11. Распоряжение Правительства РФ от 29.12.2014 N 2769-р Об утверждении Концепции региональной информатизации
12. ПП РФ от 06.07.2015 N 675 „О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 ФЗ “Об информации, информационных технологиях и о защите информации» (вместе с «Правилами …», «Правилами осуществления контроля…»)
13. ПП РФ от 06.07.2015 N 676 «О требованиях к порядку создания, развития, ввода в экспл., экспл. и вывода из эксплуатации ГИС и дальнейшего хранения содержащейся в их базах данных инф-и»
14. ПП РФ от 14.11.2015 N 1235 «О ФГИС координации информатизации» (вместе с «Положением…»)
15. ПП РФ от 31.05.2021 N 844 «Об утв. Правил внесения абонентом — юр.лицом либо ИП в ФГИС „Единая система идент. и аутент. в инфраструктуре, обеспечивающей инф.-техн. взаимодействие ИС, используемых для предоставления гос. и мун. услуг в эл. форме“ сведений, позволяющих идент-ть абонента — юр.лица либо ИП или их пользовательское (оконечное), оборудование и установления состава указанных сведений»
16. ПП РФ от 02.09.2021 N 1472 «Об определении ИС, включенных в инфраструктуру, обеспечивающую инф.-технол. взаимодействие ИС, используемых для предоставления гос. и мун. услуг и исполнения гос. и мун. функций в эл. форме, с использованием которых осуществляется инф-ое взаимодействие фед. органа исп. власти, уполн-го Прав. РФ на осущ-ие гос. кадастрового учета, гос. регистрации прав, ведение Единого гос. реестра недв. и предоставление сведений, содержащихся в ЕГРН, и депозитария, осуществляющего хранение эл. закладной или обездвиженной документарной закладной, и о внесении изменения в Положение об инфраструктуре…»

Комментарий. О «Госчейн» и «Мастерчейн».

1. ПП РФ от 22.12.2021 N 2389 «О проведении эксперимента по регистрации граждан РФ в ФГИС „ЕСИА в инфраструктуре, обеспечивающей инф.-технол. взаимодействие ИС, используемых для предоставления гос. и мун. услуг в электронной форме“ с использованием мобильного приложения» (вместе с «Положением…»)
2. ПП РФ от 13.05.2022 N 860 «О проведении эксперимента по повышению уровня защищенности ГИС фед. органов исп. власти и подвед. им учреждений» (вместе с «Положением…»)
3. ПП РФ от 28.06.2022 N 1152 «О внесении изменений в некоторые акты Прав. РФ в части создания, эксплуатации и развития ФГИС „Единая система предоставления гос. и мун. услуг (сервисов)“
4. ПП РФ от 26.08.2022 N 1498 „Об утв. требований к гос. органам для прохождения ими аккредитации на право владения ГИС, с применением которых осуществляется идентификация и (или) аутентификация, и (или) осуществления функций операторов указанных ГИС и Правил…
5. Пр. Минкомсвязи РФ от 25.08.2009 N 104 „Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования“ (Зарег. в Минюсте РФ 25.09.2009 N 14874)
6. Пр. Минкомсвязи России от 31.05.2013 N 127 „Об утверждении методических указаний по осуществлению учета ИС и компонентов инф. –телеком. инфраструктуры“ (Зарег. в Минюсте России 05.11.2013 N 30318)
7. Пр. Минкомсвязи России от 27.06.2013 N 149 „Об утв. Требований к технол., программным и лингвистическим средствам, необходимым для размещения инф-и гос. органами и органами местного самоуправления в сети “Интернет» в форме открытых данных, а также для обеспечения ее использования" (Зарег. в Минюсте России 16.08.2013 N 29414)
8. Пр. Минкомсвязи России от 22.08.2013 N 220 «Об утверждении метод. рекомендаций для исп. органов гос. власти субъектов РФ по осущ. учета и классификации ИС и компонентов инф. –телеком. инфраструктуры, создаваемых и приобретаемых за счет средств бюджетов субъектов РФ, а также по составу сведений, размещаемых в системе учета ИС»
9. Пр. Минкомсвязи России от 07.12.2015 N 514 «Об утверждении порядка внесения сведений в реестр территориального размещения технических средств ИС и формы акта о выявленных несоответствиях сведений, содержащихся в реестре» (Зарег. в Минюсте России 19.02.2016 N 41157)
10. Постановление ЦИК России от 08.06.2022 N 86/715-8 «О Требованиях к проведению дистанционного электронного голосования»

Комментарий. Документ определяет требования по защите информации, а также категории ГИС, создаваемых информационных систем.

**Государственные и муниципальные информационные системы. СМЭВ**

Пр. Минкомсвязи России от 23.06.2015 N 210 «Об утверждении Технических требований к взаимодействию информационных систем в Есистеме межведомственного электронного взаимодействия» (Зарег.в МЮ 25.08.2015 N 38668)

**Государственные и муниципальные ИС. Обеспечение безопасности**

1. Пр. ФСБ РФ N 416, ФСТЭК РФ N 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в ИС общего пользования (Зарег. в Минюсте РФ 13.10.2010 N 18704)
2. Пр. ФСТЭК России от 11.02.2013 N 17 „Об утверждении Требований о защите информации, не составляющей ГТ, содержащейся в ГИС“ (Зарег. в Минюсте России 31.05.2013 N 28608)
3. »Методический документ. Меры защиты информации в ГИС" (утв. ФСТЭК России 11.02.2014)
4. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от 6 марта 2015 г. N 240/22/879 «О банке данных угроз безопасности информации»
5. ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ФСТЭК России от от 22 июня 2017 г. № 240/22/3031 «О порядке рассмотрения и согласования моделей угроз безопасности информации и технических заданий на создание ГИС»
6. ФСТЭК России. Методика определения угроз безопасности информации в ИС (ПРОЕКТ)

**Подключение к Интернет государственных систем**

1. Указ Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению ИБ РФ при использовании ИТС международного информационного обмена»
2. Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах ИБ РФ» (вместе с «Порядком подключения ИС и ИТС к ИТС „Интернет“ и размещения (публикации) в ней информации через российский государственный сегмент ИТС „Интернет“)
3. Пр. ФСО России от 07.09.2016 N 443 „Об утверждении Положения о российском государственном сегменте ИТС “Интернет» (Зарег. в Минюсте России 14.10.2016 N 44039)

**Критическая информационная инфраструктура (КИИ)**

1. N 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ»
2. Указ Президента РФ от 30.03.2022 N 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»
3. «Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ» (утв. Президентом РФ 03.02.2012 N 803)
4. ПП РФ от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
5. ПП РФ от 17.02.2018 N 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности ЗО КИИ РФ»
6. ПП РФ от 13.04.2019 N 452 «О внесении изменений в ПП РФ от 8.02.2018 № 127»
7. ПП РФ от 08.06.2019 N 743 «Об утверждении Правил подготовки и использования ресурсов Есети электросвязи РФ для обеспечения функционирования ЗО КИИ»
8. ПП РФ от 22.08.2022 N 1478 «Об утверждении требований к ПО, в том числе в составе ПАК, используемому органами гос. власти, заказчиками, осуществляющими закупки в соответствии с ФЗ „О закупках товаров, работ, услуг отд. видами юр. лиц“ (за искл. орг. с мун. участием), на принадлежащих им ЗО КИИ РФ, Правил согласования закупок иностранного ПО (в т.ч. в с.ПАК), в целях его использования заказчиками…, а также закупок услуг, необходимых для использования этого ПО на таких объектах, и Правил перехода на преимущественное использование российского ПО (в т.ч. в с.ПАК)»
9. Пр. ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению ЗИ в АСУ производственными и ТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (Зарег. в Минюсте России 30.06.2014 N 32919)
10. Пр. ФСТЭК России от 06.12.2017 N 227 «Об утверждении Порядка ведения реестра ЗО КИИ РФ (Зарег. в Минюсте России 08.02.2018 N 49966)
11. Пр. ФСТЭК России от 11.12.2017 N 229 „Об утв. формы акта проверки, составляемого по итогам проведения гос. контроля в обл. обесп. без-ти ЗО КИИ РФ“ (Зарег. в МЮ России 28.12.2017 N 49500)
12. Пр. ФСТЭК России от 21.12.2017 N 235 „Об утв. Требований к созданию систем без-ти ЗО КИИ РФ и обеспечению их функц-ия“ (Зарег. в Минюсте России 22.02.2018 N 50118)
13. Пр. ФСТЭК России от 22.12.2017 N 236 „Об утв. формы направления сведений о рез-ах присвоения объекту КИИ одной из катег. знач-ти либо об отсутствии необх-ти присв-ия ему одной из таких кат.“ (Зарег. в МЮ России 13.04.2018 N 50753)
14. Пр. ФСТЭК России от 25.12.2017 N 239 „Об утв. Требований по обесп. без-ти ЗО КИИ РФ “ (Зарег. в МЮ России 26.03.2018 N 50524)
15. ИНФ. СООБЩЕНИЕ ФСТЭК России от 4 мая 2018 г. № 240/22/2339 о метод. доку-ах по вопросам обесп. без-ти инф-ии в ключевых системах инф. инфраструктуры РФ
16. ИНФ. СООБЩЕНИЕ ФСТЭК России от 24 августа 2018 г. № 240/25/3752 по вопросам представления перечней об. КИИ, подлежащих категорированию, и направления сведений о рез-ах присвоения объекту КИИ одной из кат. значимости либо об отсутствии необх-ти присв-ия ему одной из таких кат.
17. Инф. сообщение ФСТЭК России от 17.04.2020 N 240/84/611 „По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий“
18. Пр. ФСТЭК России от 28.05.2020 N 75 „Об утверждении Порядка согласования субъектом КИИ РФ с ФСТЭК подключения ЗОКИИ РФ к сети связи общего пользования“ (Зарег. 15.09.2020 № 59866)

**Критическая информационная инфраструктура. Связь**

1. Ассоциация документированной электросвязи. Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи.
2. Пр. Минкомсвязи России от 17.03.2020 N 114 „Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации“ (Зарег.в МЮ 25.06.2020 N 58753)

**Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)**

Комментарий. Основным федеральным законом по ГосСОПКА является N 187-ФЗот 26.07.2017. Применение ГосСОПКА тесно связанно с защитой критической информационной инфраструктуры, но в общем случае шире этой задачи.

1. «Выписка из Концепции ГосСОПКА на информационные ресурсы РФ» (утв. Президентом РФ 12.12.2014 N К 1274)
2. Указ Президента РФ от 22.12.2017 N 620 «О совершенствовании ГосСОПКА на информационные ресурсы РФ»
3. ПП РФ от 17.09.2022 N 1636 «Об утверждении Правил предоставления субсидии из фед. бюджета на создание и обеспечение деятельности отраслевого центра компетенций по ИБ в промышленности»
4. Пр. ФСБ России от 24.07.2018 N 366 «О Нац. коорд-ом центре по комп. инц-ам» (вместе с «Положением …») (Зарег.в МЮ 06.09.2018 N 52109)
5. Пр. ФСБ России от 24.07.2018 N 367 «Об утв. Перечня инф-и, предст-ой в ГосСОПКА на инф. ресурсы РФ и Порядка предст. …» (Зарег.в МЮ 06.09.2018 N 52108)
6. Пр. ФСБ России от 24.07.2018 N 368 «Об утв. Порядка обмена инф-ей о КИ между субъектами КИИ РФ, между субъектами КИИ РФ и уполн. органами ин. государств, м/н , м/н неправ. орг-ми и ин. орг-ми, осущ-ми деят-ть в области реаг. на КИ, и Порядка получ-я суб. КИИ РФ инф-ии о средствах и способах проведения комп. атак и о методах их предупр. и обнар-я» (МЮ 06.09.2018 N 52107)
7. Пр. ФСБ России от 06.05.2019 N 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий комп. атак и реагирования на КИ» (Зарег. 31.05.2019 № 54801)
8. Пр. ФСБ России от 19.06.2019 N 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий комп. атак и реагирования на КИ, за исключением средств, предназначенных для поиска признаков комп. атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ» (Зарег.в МЮ 16.07.2019 N 55285)
9. Пр. ФСБ России от 19.06.2019 N 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗО КИИ РФ» (Зарег.в МЮ 16.07.2019 N 55284)

**Персональные данные (ПДн)**

1. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физ.лиц при автоматизированной обработке ПДн » от 19.12.2005
2. N 152-ФЗ от 27.07.2006 «О ПДн»
3. N 123-ФЗ от 24.04.2020 «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий ИИ в субъекте РФ — Москве и внесении изм. в ст. 6 и 10 ФЗ „О ПДн “
4. N 168-ФЗ от 08.06.2020 „О едином федеральном информационном регистре, содержащем сведения о населении РФ “
5. Указ Президента РФ от 30.05.2005 N 609 „Об утв. Положения о ПДн гос. гражд. служащего РФ и ведении его личного дела“
6. Указ Президента РФ от 29.12.2012 N 1709 „О паспорте гражд.РФ, удостоверяющем личность за пределами территории РФ, содержащем на электронном носителе информации доп. биом. ПДн его владельца“
7. Указ Президента РФ от 24.11.2014 N 735 „О сборе биом. ПДн ин. граждан и лиц без гражданства“
8. ПП РФ от 06.07.2008 N 512 „Об утв. требований к материальным носителям биом. ПДн и технологиям хранения таких данных вне ИС ПДн “
9. ПП РФ от 15.09.2008 N 687 „Об утв. Положения об особенностях обработки ПДн , осуществляемой без использования средств автоматизации“
10. ПП РФ от 29.06.2021 N 1046 „О федеральном гос. контроле (надзоре) за обработкой ПДн “ (вместе с „Положением… “)
11. Пост. Пленума Верховного Суда РФ от 15.06.2010 N 16 „О практике применения судами Закона РФ “О средствах массовой информации»

Комментарий. Постановление поясняет понятие «общественный интерес» при обработке информации, а также дает разъяснения по использованию ГК РФ Статья 152.1. «Охрана изображения гражданина».

1. Пост. Пленума Верховного Суда РФ от 23.06.2015 N 25 «О применении судами некоторых положений раздела I части первой ГК РФ»

Комментарий. Постановление поясняет применение ГК РФ Статья 152.1. «Охрана изображения гражданина».

1. Пр. Минцифры России от 29.09.2021 N 1015 «Об утв. порядка уничтожения ПДн , получ-ых в результате обезличивания, субъектом эксп. правового режима в сфере цифр.инноваций в случае прекр. статуса субъекта эксп. правового режима» (Зарег.в МЮ 29.11.2021 N 66042)
2. Пр. Роскомнадзора от 16.07.2010 N 482 «Об утв. образца формы уведомления об обработке ПДн » (вместе с «Рекомендациями по заполнению…»)
3. Пр. Роскомнадзора от 15.03.2013 N 274 «Об утв. перечня ин. государств, не являющихся сторонами Конвенции Совета Европы о защите физ. лиц при автоматизированной обработке ПДн и обеспечивающих адекватную защиту прав субъектов ПДн » (МЮ 19.04.2013 N 28212)
4. Пр. Роскомнадзора от 30.05.2017 N 94 «Об утв. метод. рекомендаций по уведомлению уполн. органа о начале обработки ПДн и о внесении изменений в ранее представленные сведения»
5. Пр. Роскомнадзора от 24.02.2021 N 18 «Об утв. требований к содержанию согласия на обработку ПДн , разр. субъектом ПДн для распр.» (МЮ 21.04.2021 N 63204)
6. Пр. Роскомнадзора от 21.06.2021 № 106 «Об утв. Правил исп-ия ИС Роскомнадзора, в том числе порядка взаимодействия субъекта ПДн с оператором» (Рег.11.08.2021 № 64602)
7. «Полож. об идент. кредит. орг-ми клиентов, предст-ей клиента, выгодопр. и бенефиц. владельцев в целях противод-ия легализации доходов, полученных прест. путем, и финанс-ию терроризма» (утв. БР 15.10.2015 N 499-П) (МЮ 04.12.2015 N 39962)
8. Пр. Росфинмониторинга от 20.05.2022 N 100 «Об утв. треб. к идент. клиентов, предст. клиента, выгодопр-ей и бенеф. владельцев, в том числе с учетом степени (уровня) риска совершения подозрительных операций» (МЮ 20.06.2022 N 68913)

Комментарий. Данные документы, пожалуй, являются единств. документами в Рос. законодательстве, устанавливающими перечень данных, необходимых для идент. физ. лиц.

1. <Разъяснения> Роскомнадзора от 14.12.2012 «Вопросы, касающиеся обработки ПДн работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадр. резерве»
2. Пр. Роскомнадзора от 24.12.2021 N 253 «Об утверждении формы проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении фед. государственного контроля (надзора) за обработкой ПДн Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами» (Зарегистрировано в Минюсте России 25.02.2022 N 67486)
3. Пр. Роскомнадзора от 05.08.2022 N 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн » (Зарегистрировано в Минюсте России 20.09.2022 N 70152) [PRAVO.GOV.RU]
4. Письмо Роскомнадзора от 29 августа 2022 г. N 08-78032 «О рассмотрении обращения»

Комментарий. Разъяснения об отнесении фотографии к биометрическим персональным данным.

**Перс. данные. Обеспечение безопасности**

1. ПП РФ от 18.09.2012 N 940 «Об утв. Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об опр-ии доп. угроз безопасности ПДн , актуальных при обработке ПДн в С ПДн , эксплуатируемых при осуществлении определенных видов деят-ти членами таких ассоциаций…, с ФСБ РФ и ФСТЭК»
2. ПП РФ от 21.03.2012 N 211 «Об утв. перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ „О ПДн “ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися гос. или мун. органами»
3. ПП РФ от 01.11.2012 N 1119 «Об утв. требований к защите ПДн при их обработке в ИС ПДн »
4. Пр. Роскомнадзора от 05.09.2013 N 996 «Об утв. требований и методов по обезличиванию ПДн » (вместе с «Требованиями…») (МЮ 10.09.2013 N 29935)
5. «Метод. рекомендации по применению пр. Роскомнадзора от 5.09.2013 N 996 „Об утверждении требований и методов по обезличиванию ПДн “ (утв. Роскомнадзором 13.12.2013)
6. Пр. ФСТЭК от 18.02.2013 N 21 „Об утверждении Состава и содержания орг. и техн. мер по обеспечению безопасности ПДн при их обработке в ИС ПДн “ (МЮ 14.05.2013 N 28375)

Комментарий. Защита ПДн в государственных и муниципальных информационных системах осуществляется в соответствии с Пр.ом ФСТЭК России от 11.02.2013 N 17.

1. Пр. ФСБ России от 10.07.2014 N 378 „Об утв. Состава и содержания орг. и техн. мер по обеспечению безопасности ПДн при их обработке в ИС ПДн с использованием средств крипт. ЗИ, необходимых для выполнения установленных ПП требований к защите ПДн для каждого из уровней защищенности“ (МЮ 18.08.2014 N 33620)
2. Метод. рекомендации по разработке норм. правовых актов, определяющих угрозы без-ти ПДн , актуальные при обработке ПДн в ИС ПДн , эксплуатируемых при осуществлении соотв. видов деятельности» (утв. ФСБ России 31.03.2015 N 149/7/2/6-432
3. ИНФ. СООБЩЕНИЕ ФСБ РФ от 15.06.2017 «О неукосн. соблюдении операторами ПДн треб-ий формуляров на СКЗИ»
4. ИНФ. СООБЩЕНИЕ ФСБ России от 21.06.2016 «О нормативно-методических документах, действующих в области обеспечения безопасности ПДн»
5. ИНФ. СООБЩЕНИЕ ФСТЭК России от 15.07.2013 N 240/22/2637 «По вопросам ЗИ и обеспечения безопасности ПДн при их обработке в ИС в связи с изданием Пр.а ФСТЭК России от 11.02.2013 N 17 „Об утв. Требований о ЗИ, не составляющей ГТ, содержащейся в ГИС “ и Пр.а ФСТЭК России от 18.02.2013 N21
6. »Базовая модель угроз безопасности ПДн при их обработке в ИСПДн " (Выписка, 69 с.) (утв. ФСТЭК РФ 15.02.2008)

**Персональные данные. Блокировка нарушителей**

Комментарий. Законодательная основа блокировки нарушителей установлена в Федеральном законе от 27.07.2006 N 149-ФЗ.

1. ПП РФ от 19.08.2015 N 857 «Об АИС „Реестр нарушителей прав субъектов ПДн “ (вместе с „Правилами создания, формирования и ведения…”
2. Пр. Роскомнадзора от 22.07.2015 N 84 «Об утв. Порядка взаимодействия оператора РНПС ПДн с провайдером хостинга и Порядка получения доступа к информации, содержащейся в РНПС ПДн , оператором связи» (МЮ 14.08.2015 N 38532)
3. Пр. Роскомнадзора от 22.07.2015 N 85 «Об утв. формы заявления субъекта ПДн о принятии мер по ограничению доступа к инф-ии, обрабатываемой с нарушением законодательства РФв области ПДн » (МЮ 17.08.2015 N 38544)

**Персональные данные. Банковская специфика**

1. <Письмо> БР от 14.03.2014 N 42-Т «Об усилении контроля за рисками, возникающими у кред. орг-ий при использовании инф-ии, содержащей ПДн»
2. Указание БРот 10.12.2015 N 3889-У «Об определении угроз безопасности ПДн , актуальных при обработке ПДн в ИСПДн » (МЮ 18.03.2016 N 41455)

**Персональные данные. Единая биометрическая система (ЕБС)**

Комментарий. Законодательная основа Ебиометрической системы установлена в N 149-ФЗ от 27.07.2006.

1. Расп. Прав.РФ от 22.02.2018 N 293-р <О возложении на ПАО м/г и м/н электрической связи «Ростелеком» функций оператора ЕИСПДн>
2. ПП РФ от 28.03.2018 N 335 «Об определении фед. органа исп. власти, осущ. регулирование в сфере идент. граждан на основе БПДн »
3. ПП РФ от 29.06.2018 N 747 «Об уст. требований к фиксированию действий при размещении в эл.форме в ЕСИА сведений, необх. для регистрации гражданина РФ в указ. системе, и иных сведений, предусм. ФЗ, а также при размещении БПДн гражданина РФ в ЕИС ПДн , обесп-ей обработку, включая сбор и хранение БПДн , их проверку и передачу инф-и о степени их соотв-ия предоставленным БПДн»
4. ПП РФ от 30.06.2018 N 772 «Об определении состава сведений, размещаемых в ЕИС ПДн , обесп-ей обработку, включая сбор и хранение, БПДн , их проверку и передачу инф-и о степени их соотв. предост-ым БПДн физ. лица, включая вид БПДн , а также о внесении изм-ий в нек. акты Прав. РФ»
5. ПП РФ от 30.09.2021 N 1657 «Об утв. Правил осущ-я фед. органом исп. власти, уполн. в обл. обесп. без-ти, и фед. органом исп. власти, уполн. в области ПДТР и технической ЗИ, контроля и надзора за вып-ем органами, орг., ИП и нотариусами, указанными в части 18.2 статьи 14.1 ФЗ „Об информации, ИТ и о ЗИ “, орг. и техн. мер по обесп. без-ти ПДн и исп-ем СЗИ»
6. ПП РФ от 11.10.2021 N 1729 „Об утв. Положения о фед. гос. контроле (надзоре) в сфере идент. и (или) аутент.“
7. ПП РФ от 15.10.2021 N 1753 „Об утв. треб. к орг. и техн. условиям осущ. МФЦ предоставления гос. и мун. услуг размещения или обновления в ЕСИА сведений, необходимых для регистрации физ. лиц в данной системе, размещения БПДн в ЕИС ПДн , обеспечивающей обработку, включая сбор и хранение, БПДн , их проверку и передачу инф-и о степени их соотв. предоставленным БПдн ФЗ, с исп-ем прогр.-техн. комплексов“
8. ПП РФ от 20.10.2021 N 1798 „Об утв. Правил осущ. Роскомнадзором и ФСБ контроля и надзора за соблюдением МФЦ предоставления гос. и мун. услуг порядка размещения и обновления БПДн в ЕИС ПДн …“
9. ПП РФ от 20.10.2021 N 1799 „Об аккредитации орг., владеющих ИС, обеспечивающими идент. и (или) аутент. с использованием БПДн ФЛ, и (или) оказывающих услуги по идент. и (или) аутент.с использованием БПДн ФЛ “ (вместе с „Правилами аккредитации …“)
10. ПП РФ от 23.10.2021 N 1815 „Об утверждении перечня случаев осуществления сбора и обработки используемых для идент. либо идент.и аут. БПДн в ИС организаций, осуществляющих идент. и (или) аутент. с исп. БПДн ФЛ…"
11. ПП РФ от 15.06.2022 N 1066 «О размещении ФЛ своих БПДн в ЕИС ПДн , обеспечивающей обработку, включая сбор и хранение, БПДн , их проверку и передачу информации о степени их соответствия предоставленным БПДнФЛ» (вместе с «Правилами размещения…»)
12. ПП РФ от 15.06.2022 N 1067 «О случаях и сроках использования БПДн , размещенных ФЛ в ЕИС ПДн , обеспечивающей обработку, включая сбор и хранение, БПДн , их проверку и передачу информации о степени их соответствия предоставленным БПДнФЛ»
13. ПП РФ от 16.06.2022 N 1089 «Об утв. Положения о ЕИС ПДн , обеспечивающей обработку, включая сбор и хранение, БПДн , их проверку и передачу информации о степени их соответствия предоставленным БПДнФЛ»
14. Пр. Минкомсвязи России от 25.06.2018 N 321 «Об утв. порядка обработки, включая сбор и хранение, параметров БПДн в целях идент., порядка размещения и обн. БПДн в ЕБС, а также требований к ИТ и техн. средствам, предн. для обработки БПДн в целях проведения идент.» (МЮ 04.07.2018 N 51532)
15. Пр. Минкомсвязи России от 25.06.2018 N 322 «Об опр-ии размера платы, взимаемой оператором ЕИСПДн , обесп. обработку, включая сбор и хранение БПДн…, за предост. банкам, соответствующим критериям, установленным 2-4 абз.п.5.7 ст.7 ФЗ №115, информации о степени соответствия БПДн ФЛ, содержащимся в указ. системе»
16. Пр. Минкомсвязи России от 25.06.2018 N 323 «Об утв. форм подтверждения соотв. ИТ и техн. средств, предн. для обработки БПДн в целях проведения идент., требованиям к ИТ и техн. средствам, предназначенным для указанных целей» (МЮ 29.06.2018 N 51497)
17. Пр. Минцифры России от 25.05.2021 N 494 «Об утв. перечня угроз без-ти, акт. при обработке БПДн , их проверке и передаче инф. о степени их соотв. предост. БПДнФЛ в ЕИС ПДн , обесп.обработку, включая сбор и хранение БПДн , их проверку и передачу инф. о степени их соотв. предост-ым БПДнФЛ, а также акт-ых при взаимодействии гос. органов, органов МС, ИП, нотариусов и орг., за искл. орг-ий фин. рынка, с указанной системой, с учетом оценки возм. вреда, пров-ой в соотв. с зд РФ о ПДн» (МЮ 15.09.2021 N 65009)
18. Пр. Минцифры России от 06.08.2021 N 816 «Об утв. методик проверки соотв-ия предост-ых БПДн ФЛ его БПДн, содержащимся в ИС, обеспечивающих идент. и (или) аутент. с исп-ем БПДн , а также об определении степени взаимного соответствия указанных БПДн , достаточной для проведения идентификации, предусмотренной № 149-ФЗ (МЮ 08.09.2021 № 64922)
19. Пр. Минцифры России от 07.07.2021 N 685 „Об определении форм подтверждения соответствия ИТ и техн. средств, предназначенных для обработки БПДн , требованиям, определенным в соответствии с п.1 ч.13 ст. 14.1 N 149-ФЗ» (МЮ 03.09.2021 N 64868)
20. Пр. Минцифры России от 01.09.2021 N 902 «Об утв.перечня угроз без-ти, актуальных при обработке БПДн , их проверке и передаче инф. о степени их соответствия предоставленным БПДнФЛ в ИС организаций, осуществляющих идент. и (или) аутент. с исп. БПДн ФЛ, за искл. ЕИСПДн , обеспечивающей обработку, включая сбор и хранение БПДн , их проверку и передачу инф. о степени их соотв. предоставленным БПДнФЛ, а также актуальных при взаимодействии госорганов, органов МС, ИП, нотариусов и организаций, за исключением организаций финансового рынка, с указанными ИС, с учетом оценки возм. вреда, …“ (МЮ 03.11.2021 N 65692)
21. Пр. Минцифры России от 10.09.2021 N 930 „Об утверждении порядка обработки, включая сбор и хранение, параметров БПДн , порядка размещения и обновления БПДн в ЕБС и в иных ИС, обеспечивающих идент. и (или) аутент. с исп. БПДн ФЛ, а также требований к ИТ и техн. средствам, предназначенным для обработки БПДн в целях проведения идент. “ (МЮ 28.10.2021 N 65621)
22. Метод. рекомендации по нейтрализации банками угроз без-ти, актуальных при обработке, включая сбор и хранение, БПДн , их проверке и передаче информации о степени их соответствия предост-ым БПдн гражданина РФ (утв. Банком России от 14.02.2019 N 4-МР)
23. ПП РФ от 11.10.2021 N 1729 „Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере идент. и (или) аутентификации“
24. Пр. Минцифры России от 19.05.2021 N 474 „Об утверждении методики расчета взимания платы за использование Еинформационной системы ПДн , обеспечивающей обработку, включая сбор и хранение БПДн , их проверку и передачу информации о степени их соответствия представленным биометрическим персональным данным физического лица“ (Зарегистрировано в Минюсте России 29.07.2021 N 64443)

**Перс. данные. Сроки хранения**

Комментарий. Сроки хранения документов по личному составу определяются N 125-ФЗ от 22 октября 2004 .

1. Пост. ФКЦБ РФ от 16.07.2003 N 03-33/пс „Об утв. Полож. о порядке и сроках хран. док-в АО “ (МЮ 21.08.2003 N 4994)
2. Пр. Росархива от 20.12.2019 N 236 „Об утв. Перечня тип. управл. арх. док-ов, образ-ся в процессе деят. госорганов, органов МС и орг-ий, с указ. сроков их хранения“ (МЮ 06.02.2020 N 57449)
3. Пр. Росархива от 28.12.2021 N 142 „Об утв. Перечня тип. арх. док-ов, образ-ся в НТ и произв-ой деят. орг-ий, с указ. сроков хран.“ (МЮ 02.02.2022 N 67095)
4. Положение Росархива N 1, Банка России N 801-П от 12.07.2022 „Об утв. Перечня док-ов, образующихся в процессе деят. кред. орг., с указанием сроков их хран.“ (МЮ 19.07.2022 N 69304)