

# Основы построения защищенных баз данных

Ваша команда по спасению компьютерной безопасности

7 мая 2022 г.

Самый надежный в мире алгоритм

Всегда делать исключительно то, что горит

В самый прекрасный последний момент

Ведь для самых важных дел в принципе лучше времени нет

---

Anacondaz - Факап

## Содержание

<b>1</b>	<b>Концепция безопасности БД</b>	<b>4</b>
1.0.1	Понятие безопасности БД	4
1.0.2	Угрозы безопасности БД: общие и специфичные	6
1.0.3	Требования безопасности БД	10
1.0.4	Защита от несанкционированного доступа	13
1.0.5	Защита от вывода	14
1.0.6	Целостность БД	14
1.0.7	Аудит	15
1.0.8	Многоуровневая защита	16
1.0.9	Типы контроля безопасности: потоковый, контроль вывода, контроль доступа	17
<b>2</b>	<b>Теоретические основы безопасности в СУБД</b>	<b>19</b>
2.1	Критерии защищенности БД	19
2.1.1	Критерии оценки надежных компьютерных систем (TCSEC)	19
2.1.2	Понятие политики безопасности	20
2.1.3	Совместное применение различных политик безопасности в рамках единой модели	20
2.1.4	Интерпретация TCSEC для надежных СУБД (TDI)	21
2.1.5	Оценка надежности СУБД как компоненты вычислительной системы	21
2.1.6	Монитор ссылок	21
2.1.7	Применение TCSEC к СУБД непосредственно	21
2.1.8	Элементы СУБД, к которым применяются TDI: метки, аудит, архитектура системы, спецификация, верификация, проектная документация	21
2.1.9	Критерии безопасности ГТК	21

2.2	Модели безопасности в СУБД . . . . .	21
2.2.1	Аспекты исследования моделей безопасности . . . . .	23
2.2.2	Классификация моделей безопасности . . . . .	23
2.2.3	Дискреционная модель . . . . .	24
2.2.4	Мандатная модель . . . . .	29
2.2.5	Ролевая модель . . . . .	37
2.2.6	Особенности реализации моделей безопасности в СУБД . . . . .	37
<b>3</b>	<b>Механизмы обеспечения целостности СУБД</b>	<b>42</b>
3.1	Угрозы целостности СУБД . . . . .	42
3.2	Метаданные и словарь данных . . . . .	44
3.3	Понятие транзакции . . . . .	47
3.4	Блокировки . . . . .	51
3.5	Ссылочная целостность . . . . .	54
3.6	Правила(триггеры) . . . . .	58
3.7	События . . . . .	59
<b>4</b>	<b>Механизмы обеспечения конфиденциальности в СУБД</b>	<b>60</b>
4.1	Классификация угроз конфиденциальности СУБД . . . . .	60
4.1.1	Причины, виды, основные методы нарушения конфиденциальности . . . . .	60
4.1.2	Типы утечки конфиденциальной информации из СУБД, частичное разглашение	62
4.1.3	Соотношение защищенности и доступности данных . . . . .	63
4.1.4	Получение несанкционированного доступа к конфиденциальной информации путем логических выводов . . . . .	63
4.1.5	Методы противодействия. Особенности применения криптографических методов	65
4.1.6	Применение шифрования в базах данных . . . . .	66
4.2	Средства идентификации и аутентификации . . . . .	67
4.2.1	Общие сведения . . . . .	67
4.2.2	Совместное применение средств идентификации и аутентификации, встроен- ных в СУБД и в ОС . . . . .	69
4.3	Средства управления доступом . . . . .	70
4.3.1	Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. . . . .	70
4.3.2	Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. . . . .	70
4.3.3	Соотношение прав доступа СУБД и операционной системы . . . . .	71
4.3.4	Метки безопасности. . . . .	72
4.3.5	Использование представлений для обеспечения конфиденциальности инфор- мации в СУБД. . . . .	73
4.4	Обеспечение конфиденциальности путем тиражирования БД . . . . .	74
4.5	Аудит и подотчетность . . . . .	75
4.5.1	Подотчетность действий пользователя и аудит связанных с безопасностью со- бытий. . . . .	75
4.5.2	Регистрация действий пользователя . . . . .	76

4.5.3	Управление набором регистрируемых событий . . . . .	77
4.5.4	Анализ регистрационной информации . . . . .	77
<b>5</b>	<b>Механизмы, поддерживающие высокую готовность</b>	<b>78</b>
5.1	Средства, поддерживающие высокую готовность . . . . .	79
5.2	Оперативное администрирование . . . . .	82
5.3	Функциональная насыщенность СУБД . . . . .	84
5.4	Системы, обладающие свойством высокой готовности . . . . .	85
<b>6</b>	<b>Защита данных в распределенных системах</b>	<b>86</b>
6.1	Распределенные вычислительные среды . . . . .	86
6.2	Угрозы безопасности распределенных СУБД . . . . .	87
6.3	Распределенная обработка данных . . . . .	94
6.4	Протоколы фиксации . . . . .	96
6.5	Тиражирование данных . . . . .	99
6.6	Интеграция БД и Internet . . . . .	101
<b>7</b>	<b>Безопасность в статистических БД</b>	<b>101</b>
7.1	Общие сведения . . . . .	102
7.2	Классификация . . . . .	102
7.3	Угрозы статистических БД . . . . .	103
7.4	Защита в статистических БД . . . . .	104
<b>8</b>	<b>Распознавание вторжений в БД</b>	<b>106</b>
8.1	Основные понятия . . . . .	106
8.2	Системы распознавания вторжений . . . . .	107
8.2.1	Типы моделей систем распознавания вторжений (ID-систем) . . . . .	107
8.2.2	Общая структура ID-систем . . . . .	108
8.2.3	Шаблоны классов пользователей . . . . .	109
8.2.4	Модели известных атак . . . . .	110
8.3	Экспертные ID-системы . . . . .	111
8.3.1	Метрики . . . . .	111
8.3.2	Статистические модели . . . . .	111
8.3.3	Профили . . . . .	112
8.3.4	Примеры ID-систем . . . . .	112
8.4	Развитие систем распознавания вторжений . . . . .	114
8.4.1	Развитие практических аспектов СОВ . . . . .	114
8.4.2	Развитие теоретических аспектов СОВ . . . . .	114
<b>9</b>	<b>Проектирование безопасности БД</b>	<b>115</b>
9.1	Основные понятия . . . . .	115
9.2	Методология проектирования . . . . .	116
9.2.1	Отличия в проектировании безопасных ОС и СУБД . . . . .	116
9.2.2	Основные требования к безопасности СУБД . . . . .	116
9.2.3	Независимые принципы целостности данных . . . . .	117

9.2.4	Модель авторизации в System R	118
9.2.5	Архитектура безопасной СУБД	118
9.3	Проектирование безопасных БД	121
9.3.1	Фазы проектирования безопасных БД (по DoD)	123
9.3.2	Предварительный анализ	124
9.3.3	Требования и политики безопасности	125
9.3.4	Концептуальное проектирование	127
9.3.5	Логическое проектирование	128
9.3.6	Физическое проектирование	141
9.4	Формальные верификации и спецификации	142

## 1 Концепция безопасности БД

### 1.0.1 Понятие безопасности БД

Для того чтобы иметь общую точку старта нам придется дать пару определений, я постараюсь быстро разобраться с обязательной копипастой и перейти к делу. Итак:

**База данных**<sup>1</sup> – это организованная коллекция данных, обычно хранящихся и доступных в электронном виде из компьютерной системы. Там, где базы данных более сложны, они часто разрабатываются с использованием формальных методов проектирования и моделирования.

**Система управления базами данных (СУБД)**<sup>1</sup> – это программное обеспечение, которое взаимодействует с конечными пользователями, приложениями и самой базой данных для сбора и анализа данных. Программное обеспечение СУБД дополнительно включает в себя основные средства, предоставляемые для администрирования базы данных. Общая сумма базы данных, СУБД и связанных приложений может называться «системой базы данных». Часто термин «база данных» также используется для обозначения любой СУБД, системы баз данных или приложения, связанного с базой данных.

Но если вас вдруг спросят, то смело отвечайте:

Согласно **гражданскому кодексу** Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 18.07.2019), базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

И если с просто базами данных все более-менее понятно, то в тот момент, когда нам приходится говорить о вопросах безопасности, все превращается в классическую задачу о двух стульях: как надо

<sup>1</sup>Нагло скопипизированно с **вечно загнивающей**

и как в законе написано. (Ну или пафосно перефразируя) Вопросы информационной безопасности баз данных целесообразно рассматривать с двух взаимодополняющих позиций (**Lihonosov2011**)<sup>2</sup>:

- оценочные стандарты, направленные на классификацию информационных систем и средств их защиты по требованиям безопасности
- технические спецификации, регламентирующие различные аспекты реализации средств защиты

Попытка защищать все и сразу обречена на провал, так что довольно логичным кажется сосредоточиться на обеспечении безопасности четырех уровней информационной системы (**Lihonosov2011**) :

1. уровня прикладного программного обеспечения, отвечающего за взаимодействие с пользователем
2. уровня системы управления базами данных, обеспечивающего хранение и обработку данных информационной системы
3. уровня операционной системы, отвечающего за функционирование СУБД и иного прикладного программного обеспечения
4. уровня среды доставки, отвечающего за взаимодействие информационных серверов и потребителей информации

Теперь уже можно ввести недостающие определения. Я вижу как вы соскучились по определениям<sup>3</sup>.

Если БД рассматривать только как совокупность данных, то можно использовать следующее определение:

- **Безопасность информации [данных]**: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.
- **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Если БД рассматривать как информационную систему, то можно использовать следующие определения:

- **Безопасность ИС (БД)** можно определить как состояние защищенности ИС от угроз ее нормальному функционированию. Под защищенностью понимается наличие средств ИС и методов их применения, обеспечивающих снижение или ликвидацию негативных последствий, связанных с реализацией угроз. Изложенный подход к определению понятия безопасности ИС предполагает, что перечень и содержание угроз достаточно хорошо определены и достаточно стабильны во времени.

<sup>2</sup>Мне стыдно указывать ресурс, где я взял этот кусок, так что пусть будет [pornhub](#)

<sup>3</sup>А эти определения я взял с прошлого года

- **Безопасность ИС (БД)** можно определить как свойство системы адаптироваться к агрессивным проявлениям среды, в которой функционирует система, обеспечивающее поддержку на экономически оправданном уровне характеристики качества системы. В сформулированном определении основной акцент делается не на перечне и содержании угроз, нейтрализация которых обеспечивается, а на особую характеристику качества системы. При этом основной критерий качества ИС является экономическим, т.е. оценка средств и методов обеспечения безопасности осуществляется на основе затрат на реализацию механизмов безопасности и потенциальных выгод от недопущения ущерба, связанного с целенаправленным или случайным агрессивным проявлением среды.

Ну и не одно введение не может обойтись без заклинания

Проблема обеспечения безопасности автоматизированных информационных систем может быть определена как решение трех взаимосвязанных задач по реализации требуемого уровня:

- **конфиденциальности** – обеспечения пользователям доступа только к данным, для которых пользователь имеет явное или неявное разрешение на доступ
- **целостности** – обеспечения защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки
- **доступности** – обеспечения возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией

### 1.0.2 Угрозы безопасности БД: общие и специфичные

Интуитивное понимание угрозы безопасности можно сформулировать как нарушение велико-  
лепной тройки: ~~Труе, Балбее и Бывальнй~~ конфиденциальность, целостность, доступность. Для формального диалога можно использовать что-то около<sup>4</sup>:

**Угрозой информационной безопасности** автоматизированный информационной системе (АИС) назовем возможность воздействия на информацию, обрабатываемую в системе, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты информационной системы, приводящего к утрате, уничтожению или сбою функционирования носителя информации или средства управления программно-аппаратным комплексом системы.

Для того, чтобы разобраться во всем зоопарке перечисленных воздействий на систему нам придется все это дело классифицировать. Для удобства будем сразу смотреть на это со стороны об-  
роняющего, то есть по источнику воздействия. В этом контексте они довольно естественно разби-

<sup>4</sup>Нагло взято [отсюда](#)

ваются на внутренние и внешние. Для описания внешних угроз необходимо учитывать объекты воздействия. (Под объектами воздействия понимаются объекты, которые могут подвергнуться атакам или могут стать причиной их возникновения.) (Ytebov2008)

Внешними дестабилизирующими факторами, создающими угрозы безопасности функционированию систем баз данных и СУБД, являются:

- умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы, причиной которых являются нарушения информационной безопасности защищаемого объекта
- искажения в каналах передачи информации, поступающей от внешних источников, циркулирующих в системе и передаваемой потребителям, а также недопустимые значения и изменения характеристик потоков информации из внешней среды и внутри системы
- сбои и отказы в аппаратуре вычислительных средств
- вирусы и иные деструктивные программные элементы, распространяемые с использованием систем телекоммуникаций, обеспечивающих связь с внешней средой или внутренние коммуникации распределенной системы баз данных
- изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределы, проверенные при тестировании или сертификации системы

Внутренними источниками угроз безопасности баз данных и СУБД являются:

- системные ошибки при постановке целей и задач проектирования автоматизированных информационных систем и их компонент, допущенные при формулировке требований к функциям и характеристикам средств обеспечения безопасности системы
- ошибки при определении условий и параметров функционирования внешней среды, в которой предстоит использовать информационную систему и, в частности, программно-аппаратные средства защиты данных
- ошибки и несанкционированные действия пользователей, административного и обслуживающего персонала в процессе эксплуатации системы
- недостаточная эффективность используемых методов и средств обеспечения информационной безопасности в штатных или особых условиях эксплуатации системы

Если у вас разбегаются глаза, это нормально – здесь перечислены атаки на всех уровнях . Что за уровни? Напоминаю:

- На уровне сети
  - Activex-объект
  - Интерфейсы: OLE DB, ADO, ODBC, JDBC
  - Протоколы: TCP/IP, IPX/SPX, Named Pipes, Multiprotocol
  - Рабочие станции
  - Серверы

- Маршрут
- URL
- На уровне ОС
  - Аппаратное обеспечение
  - Программное обеспечение
  - Файлы базы данных
  - Файлы журнала транзакций
  - Файлы резервного копирования
  - Transact-SQL, PLSQL
  - Службы: MSSQLServer, SQLServerAgent, TNSListener и т. д.
- На уровне БД
  - Пользователи
  - Роли
  - Роли приложения
  - Диаграммы
  - Представления
  - Таблицы
  - Хранимые процедуры
  - Определения по умолчанию
  - Правила
  - Функции
  - Тип данных

Дальше, также легко и непринужденно можно разбить все атаки на СУБД на:

1. атаки на уровне ОС
2. атаки на уровне сети
3. атаки на уровне БД

Атаки на ОС, в которых функционирует СУБД, возникают гораздо чаще, так как защитить ОС гораздо сложнее, чем СУБД. Это обусловлено тем, что число различных типов защищаемых объектов в современных ОС может достигать нескольких десятков, а число различных типов защищаемых информационных потоков – нескольких сотен. Возможность практической реализации той или иной атаки на ОС в значительной мере определяется архитектурой и конфигурацией ОС. Тем не менее существуют атаки, которые могут быть направлены практически на любые ОС:

1. Кража ключевой информации (паролей)



2. Подбор пароля
3. Сканирование жестких дисков компьютера
4. Превышение полномочий
5. Атаки класса «Отказ в обслуживании»

Наиболее опасные атаки на СУБД исходят из сетей. На уровне сетевого программного обеспечения возможны следующие атаки на СУБД:

1. Прослушивание канала
2. Перехват пакетов на маршрутизаторе
3. Создание ложного маршрутизатора
4. Навязывание пакетов
5. Атаки класса «Отказ в обслуживании»

Теперь спускаемся на уровень самой БД. Для простоты восприятия разобьем все кучкам угроз конфиденциальности, целостности и доступности (Опять же, согласно (Ytebov2008)):

- К угрозам конфиденциальности информации можно отнести следующие :
  1. Инъекция SQL. Во многих приложениях используется динамический SQL – формирование SQL-предложений кодом программы путем конкатенации строк и значений параметров. Зная структуру базы данных, злоумышленник может либо выполнить хранимую программу в запросе, либо закомментировать «легальные» фрагменты SQL-кода, внедрив, например, конструкцию UNION, запрос которой возвращает конфиденциальные данные. В последнее время злоумышленник может использовать специальные программы, автоматизирующие процесс реализации подобных угроз.
  2. Логический вывод на основе функциональных зависимостей. Пусть дана схема отношения:  $R(A_1, \dots, A_n)$ . Пусть  $U = \{A_1, \dots, A_n\}$ ,  $X, Y$  – подмножества из  $U$ .  $X$  функционально определяет  $Y$ , если в любом отношении  $r$  со схемой  $R(A_1, \dots, A_n)$  не могут содержаться два кортежа с одинаковыми значениями атрибутов из  $X$  и с различными из  $Y$ . В этом случае имеет место функциональная зависимость, обозначаемая  $X \Rightarrow Y$ . В реальных БД при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.
  3. Логический вывод на основе ограничений целостности. Для кортежей отношений в реляционной модели данных можно задать ограничения целостности – логические условия, которым должны удовлетворять атрибуты кортежей. При этом ограничение целостности может быть задано в виде предиката на всем множестве атрибутов кортежа. В случае попытки изменить данные в таблице, СУБД автоматически вычисляет значение этого предиката, и в зависимости от его истинности операция разрешается или отвергается. Многократно изменяя данные и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него нет непосредственного доступа. К этому виду угроз можно отнести также анализ значений первичных/вторичных ключей.

4. Использование оператора UPDATE для получения конфиденциальной информации. В некоторых стандартах SQL пользователь, не обладая привилегией на выполнение оператора SELECT, мог выполнить оператор UPDATE со сложным логическим условием. Так как после выполнения оператора UPDATE сообщается, сколько строк он обработал, фактически пользователь мог узнать, существуют ли данные, удовлетворяющие этому условию.
- К угрозам целостности информации, специфические для СУБД можно отнести следующие :
    1. С помощью SQL-операторов UPDATE, INSERT и DELETE можно изменить данные в СУБД. Опасность заключается в том, что пользователь, обладающий соответствующими привилегиями, может модифицировать все записи в таблице.
  - К угрозам доступности для СУБД можно отнести следующие:
    1. Использование свойств первичных и внешних ключей. В первую очередь отнесем сюда свойство уникальности первичных ключей и наличие ссылочной целостности. В том случае, если используются натуральные, а не генерируемые системой значения первичных ключей, может создаться такая ситуация, когда в таблицу невозможно будет вставить новые записи, так как там уже будут записи с такими же значениями первичных ключей. Если в БД поддерживается ссылочная целостность, можно организовать невозможность удаления родительских записей, умышленно создав подчиненные записи.
    2. Блокировка записей при изменении. Заблокировав записи или всю таблицу, злоумышленник может на значительное время сделать ее недоступной для обновления.
    3. Загрузка системы бессмысленной работой. Злоумышленник может выполнить запрос, содержащий декартовое произведение двух больших отношений. Мощность декартового произведения двух отношений мощности  $N_1$  и  $N_2$  равна  $N_1 \cdot N_2$ . Это означает, что при выдаче злоумышленником запроса вида `SELECT * FROM Tab1, Tab1 ORDER BY 1`, где мощность отношения (количество строк в таблице Tab1)  $N_1 = 10000$ , мощность результирующего отношения будет  $N = N_1^2 = 10000^2$ . Вычисление соединения и сортировка результирующего отношения потребуют значительных ресурсов системы и отрицательно скажутся на производительности операций других пользователей.
    4. Использование разрушающих программных средств. Например, атака типа «троянский конь» – запуск пользователями программ, содержащих код, выполняющий определенные действия, внедренный туда злоумышленником.

### 1.0.3 Требования безопасности БД

Если сильно постараться то, на основании угроз можно выделить следующий список требований к безопасности БД<sup>5</sup>:

- Функционирование в доверенной среде. Под доверенной средой следует понимать инфраструктуру предприятия и ее защитные механизмы, обусловленные политиками безопасности. Таким образом, речь идет о функционировании СУБД в соответствии с правилами безопасности, применяемыми и ко всем прочим системам предприятия

---

<sup>5</sup>За оригиналом [сюда](#)

- Организация физической безопасности файлов данных. Требования к физической безопасности файлов данных СУБД в целом не отличаются от требований, применяемых к любым другим файлам пользователей и приложений
- Организация безопасной и актуальной настройки СУБД. Данное требование включает в себя общие задачи обеспечения безопасности, такие как своевременная установка обновлений, отключение неиспользуемых функций или применение эффективной политики паролей
- Безопасность пользовательского ПО. Сюда можно отнести задачи построения безопасных интерфейсов и механизмов доступа к данным
- Безопасная организация и работа с данными. Вопрос организации данных и управления ими является ключевым в системах хранения информации. В эту область входят задачи организации данных с контролем целостности и другие, специфичные для СУБД проблемы безопасности. Фактически эта задача включает в себя основной объем зависящих от данных уязвимостей и защиты от них

Но настало время отставить логику в сторону и поговорить на эльфийском о юридических требованиях. В целом, в России пытаются регламентировать эту отрасль, но в основном это басни про «кругом враги», «безопасная безопасность» и «импортозамещать до потери пульса». Даже «вертикаль власти» не забыли [(Mysev2019)].<sup>6</sup>

Для беглого ознакомления достаточно заглянуть в [ФЗ «Об информации, информационных технологиях и о защите информации»](#) и в [Указ президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»](#). Хотя что-то более-менее содержательное начинается с [требований ФСТЭК](#).

Итак, согласно ФСТЭК у автоматизированная система управления, имеет многоуровневую структуру :

1. уровень операторского (диспетчерского) управления (верхний уровень)
2. уровень автоматического управления (средний уровень)
3. уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень)

В автоматизированной системе управления объектами защиты являются:

1. информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса
2. программно-технический комплекс, включающий технические средства, программное обеспечение, а также средства защиты информации

Принимаемые организационные и технические меры защиты информации:

- должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтоже-

<sup>6</sup>Если очень хочется, то можно преисполниться вот [этой монографией](#)

ния, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации)

- должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса
- не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования должны обеспечивать:

- идентификацию и аутентификацию (ИАФ)
- управление доступом (УПД)
- ограничение программной среды (ОПС)
- защиту машинных носителей информации (ЗНИ)
- аудит безопасности (АУД)
- антивирусную защиту (АВЗ)
- предотвращение вторжений (компьютерных атак) (СОВ)
- обеспечение целостности (ОЦЛ)
- обеспечение доступности (ОДТ)
- защиту технических средств и систем (ЗТС)
- защиту информационной (автоматизированной) системы и ее компонентов (ЗИС)
- реагирование на компьютерные инциденты (ИНЦ)
- управление конфигурацией (УКФ)
- управление обновлениями программного обеспечения (ОПО)
- планирование мероприятий по обеспечению безопасности (ПЛН)
- обеспечение действий в нештатных ситуациях (ДНС)
- информирование и обучение персонала (ИПО)

Для разнообразия можно ознакомиться с положением дел в Беларуси. Там есть вот такие приколные законы<sup>7</sup>:

- Об информатизации
- О научно-технической информации;
- О национальном архивном фонде и архивах в Республике Беларусь
- О печати и других средствах массовой информации
- О правовой охране программ для ЭВМ и баз данных
- О введении в действие Единой системы классификации и кодирования технико-экономической и социальной информации Республики Беларусь
- и др.

#### 1.0.4 Защита от несанкционированного доступа

Когда мы начинаем говорить о безопасности бд, в первую очередь в голову приходит мысль, что не плохо было бы подумать о конфиденциальности (а уже потом про доступность и тд.). С нее и начнем.

К основным средствам защиты информации относят следующие<sup>8</sup>:

- идентификация и аутентификации
- установление прав доступа к объектам БД
- защита полей и записей таблиц БД
- шифрование данных и программ

Простейший пример аутентификации это парольная защита. Парольная защита представляет простой и эффективный способ защиты БД от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами БД и хранятся в определенных системных файлах СУБД в зашифрованном виде. Улучшенным вариантом является использование механизма SSL-аутентификации с использованием сертификатов.

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта, а также администратор БД имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа.

К данным, имеющимся в таблице, могут применяться меры защиты по отношению к отдельным полям и отдельным записям. В реляционных СУБД отдельные записи специально не защищаются. Применительно к защите данных в полях таблицы можно выделить такие уровни прав доступа, как полный запрет доступа, только чтение, разрешение всех операций (просмотр, ввод новых значений,

---

<sup>7</sup>А это взято с [лекций по администрированию баз данных](#)

<sup>8</sup>За оригиналом [сюда](#)

удаление, изменение). Более мощным средством защиты данных является их шифрование. Для расшифрования информации пользователи, имеющие санкционированный доступ к зашифрованным данным, имеют ключ и алгоритм расшифрования.

Итак, для минимизации риска несанкционированного доступа необходима реализация комплекса нормативных, организационных и технических защитных мер, в первую очередь: введение ролевого управления доступа, организация доступа пользователей по предъявлению сертификата, выборочное шифрование для сегментов базы данных.

#### 1.0.5 Защита от вывода

Мы уже говорили об этом в угрозах безопасности 1.0.2 на 9 странице. У (Ytebov2008) есть только объяснение логического вывода на основе функциональных зависимостей или ограничений целостности, а за решением нас посылают в (Smirnov2007). О! Я тут неожиданно понял что все, что я находил в интернете, в статьях и других книгах это копияста различной степени наглости из (Smirnov2007). Так что не буду отличаться оригинальностью и я. Помимо очевидного мониторинга с целью свести количество таких связей к минимуму, надо очень внимательно следить за привилегиями (принцип минимальных привилегий).

Привилегия – это разрешение на выполнение в системе определенного действия. Не имея соответствующей привилегии, пользователь не может получить доступ к данным или выполнить какое-либо действие.

Все привилегии могут быть разделены на два класса: системные привилегии и привилегии доступа к объектам.

Системная привилегия – это привилегия, которая дает пользователю право на выполнение какой-либо операции в масштабе базы данных. Например, пользователь с системной привилегией ALTER TABLESPACE может изменять любую табличную область (за исключением некоторых ограничений на табличную область SYSTEM).

Привилегия доступа к объекту – это разрешение пользователю на выполнение определенной операции над определенным объектом, например выполнение выборки из некоторой таблицы. При этом пользователь может формировать любые запросы к данной таблице, но не имеет права модифицировать данные этой таблицы или формировать какой-либо запрос к другой таблице.

#### 1.0.6 Целостность БД

Когда мы говорили о защите от НСД, речь шла о конфиденциальности. Теперь настало время целостности.

По (Smirnov2007):

Задача обеспечения целостности предусматривает комплекс мер по предотвращению непреднамеренного изменения или уничтожения информации, используемой информационной системой управления или системой поддержки принятия решений. Изменение или уничтожение данных может быть следствием неблагопри-

ятного стечения обстоятельств и состояния внешней среды (стихийные бедствия, пожары и т. п.), неадекватных действий пользователей (ошибки при вводе данных, ошибки операторов и т. п.) и проблем, возникающих при многопользовательской обработке данных.

Угроза нарушения целостности включает в себя любое умышленное или случайное изменение информации, обрабатываемой в информационной системе или вводимой из первичного источника данных. К нарушению целостности данных может привести как преднамеренное деструктивное действие некоторого лица, изменяющего данные для достижения собственных целей, так и случайная ошибка программного или аппаратного обеспечения, приведшая к безвозвратному разрушению данных.

Мы уже обсуждали основные угрозы целостности в 1.0.2 на 10.

Средства обеспечения целостности баз данных включают автоматическую поддержку некоторой системы правил, описывающих допустимость и достоверность хранимых и вводимых значений. Реляционная модель включает некоторые характерные правила, вытекающие из существа модели: ограничения домена и ограничения таблицы.

- Целостность домена предполагает, что допустимое множество значений каждого атрибута является формально определенным. То есть существуют формальные способы проверки того, что конкретное значение атрибута в базе данных является допустимым. Строка не будет вставлена в таблицу, пока каждое из значений ее столбцов не будет находиться в соответствующем домене (множестве допустимых значений).
- Целостность таблицы означает, что каждая строка в таблице должна быть уникальной. Хотя не все СУБД промышленного уровня требуют выполнения такого ограничения, возможность уникальной идентификации каждой строки представляется необходимой для большинства реальных приложений.

Ограничения целостности позволяют гарантировать, что требования к данным будут соблюдаться независимо от способа их загрузки или изменения. В большинстве СУБД предусмотрена поддержка следующих типов статических ограничений целостности<sup>9</sup>:

1. ограничение на определенность значения атрибута (NOT NULL)
2. ограничение на уникальность значения атрибутов (UNIQUE)
3. ограничение – первичный ключ
4. ограничение – внешний ключ
5. ограничение целостности, задаваемое предикатом

### 1.0.7 Аудит

Мало того, что все это великолепие надо долго и скрупулезно настраивать, так еще и за всем этим надо следить. О том, как, мы, опять же, находим у (Smirnov2007).

<sup>9</sup>Немного другая точка зрения: <https://studfiles.net/preview/6354061/page:55/> (Роскомнадзор будет ругаться, но вас это пугать не должно)

Важнейшей составляющей процесса обеспечения безопасности ИС является проведение квалифицированного аудита. Проведение профессионального независимого аудита позволяет своевременно выявить существующие недостатки в системе обеспечения безопасности ИС и объективно оценить соответствие параметров, характеризующих режим обеспечения информационной безопасности, требуемому решаемым задачам организации уровню.

Полноценная система обеспечения безопасности ИС должна обладать развитыми средствами аудита, то есть, как минимум, СУБД должна обладать средствами автоматического ведения протоколов действий пользователей системы.

В СУБД средство ведения аудита может быть реализовано в виде независимой утилиты (IBM DB2) или возможностей, управляемых языковыми средствами системы (Oracle). Средства аудита обычно ассоциированы с экземпляром, т. е. для каждого экземпляра сервера баз данных может быть запущен собственный файл аудита.

Средства аудита выполняют фиксацию информации об активности пользователей системы в словаре данных или специальном файле – журнале аудита. Информация о настройках системы аудита хранится в специальном конфигурационном файле. Файл настройки или параметры команды активизации аудита определяют перечень событий, которые фиксируются системой аудита.

Пользователь, обладающий необходимыми полномочиями, может выполнять следующие действия со средствами аудита:

- запускать и останавливать средства аудита;
- просматривать состояние конфигурации средства аудита и настраивать средства аудита на фиксацию определенных событий;
- переписывать данные аудита во внешние файлы операционной системы для проведения независимого анализа.

#### 1.0.8 Многоуровневая защита

Мы уже успели поговорить про уровни в связке интерфейс-СУБД-ОП-среда [1.0.1], сеть-ОС-БД [1.0.2] и даже ФСТЭКовские уровни [1.0.3].

Самое полное описание, пожалуй, сеть-ОС-БД, так что дальше будем отталкиваться от него. Вполне очевидно что защищать все и сразу сложно, каждый уровень имеет свою специфику, но какие то общие принципы выделить можно. Так как все труды на эту тему каскадно ссылаются на (Smirnov2007), то просто процитирую:

Анализ наиболее успешных решений в области обеспечения информационной безопасности баз данных позволил сформулировать несколько полезных принципов, которыми можно руководствоваться при проектировании систем защиты:

- экономическая оправданность механизмов защиты
- открытое проектирование
- распределение полномочий между различными субъектами в соответствии с правилами организации



- минимально возможные привилегии для пользователей и администраторов
- управляемость системы при возникновении отказов и сбоев
- психологическая приемлемость работы средств защиты данных

### 1.0.9 Типы контроля безопасности: потоковый, контроль вывода, контроль доступа

Про все три типа мы уже успели поговорить. В частности 1.0.2 и 1.0.3. Единственное, что осталось уточнить – это контроль доступа. Идейно он этот вопрос распадается на два: *кому* и *что* мы будем разрешать?

**Кому?** Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: идентификации, аутентификации и авторизации.

Общепринято, что технологии идентификации и аутентификации являются обязательным элементом защищенных систем, так как обеспечивают аксиоматический принцип персонализации субъектов и, тем самым, реализуют первый (исходный) программно-технический рубеж защиты информации в компьютерных системах.

Под идентификацией понимается различение субъектов, объектов, процессов по их моделям, существующим в форме имен. Под аутентификацией понимается проверка и подтверждение подлинности образа идентифицированного субъекта, объекта, процесса. Как вытекает из самой сути данных понятий, в основе технологий идентификации и аутентификации лежит идеология вероятностного распознавания образов, обуславливая, соответственно, принципиальное наличие ошибок первого и второго рода.

1. Сущность процедуры идентификации состоит в назначении пользователю, т. е. объекту – потребителю ресурсов сервера баз данных – имени. Имя пользователя – это некоторая уникальная метка, соответствующая принятым соглашениям именования и обеспечивающая однозначную идентификацию объекта реального мира в пространстве отображаемых объектов. С позиций ИС источники, предъявившие идентификатор, неразличимы.
2. Сущность процедуры аутентификации состоит в подтверждении подлинности пользователя, представившего идентификатор.
3. Сущность процедуры авторизации состоит в определении перечня конкретных информационных ресурсов, с которыми аутентифицированному пользователю разрешена работа.

Процедуры идентификации, аутентификации и авторизации являются обязательными для любой защищенной ИС.

**Что?** В целом используют одну из трех моделей безопасности: дискреционная, мандатная и ролевая.

1. Простейшая (одноуровневая) модель безопасности данных строится на основе дискреционного (избирательного) принципа разграничения доступа, при котором доступ к объектам осуществляется на основе множества разрешенных отношений доступа в виде троек – «субъект доступа – тип доступа – объект доступа».

Наглядным и распространенным способом формализованного представления дискреционного доступа является матрица доступа, устанавливающая перечень пользователей (субъектов) и перечень разрешенных операций (процессов) по отношению к каждому объекту базы данных (таблицы, запросы, формы, отчеты).

2. Мандатная модель доступа характерна для случая, когда возможность конкретных действий с данными или документами определяется внешним, обычно глобальным собственником информации. Исторически в роли такого глобального собственника чаще всего выступало государство. Основная идея мандатной модели доступа состоит в приписывании объектам и субъектам доступа меток. Если метки объекта и субъекта соответствуют (в некотором смысле), то субъект получает право на выполнение определенных действий с объектом. В роли метки, приписываемой субъектам в государственных структурах, выступает, например, форма допуска. В реляционной модели в качестве структуры, обладающей меткой, естественно выбрать кортеж.
3. В основу ролевой модели положена идея принадлежности всех данных системы некоторой организации, а не пользователю, как в случае моделей дискреционного и мандатного доступа. В целом модель ориентирована на упрощение и обеспечение формальной ясности в технологии обеспечения политики безопасности системы. Управление доступом в ролевой модели осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов.

В ролевой модели классическое понятие субъект разделяется на две части: пользователь и роль. Пользователь — это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль — это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор привилегий, необходимых для осуществления определенной деятельности. (Самым распространенным примером роли является присутствующая почти в каждой системе учетная запись администратора (например, root для UNIX и Administrator для Windows), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая модель включает три компонента: модель отображения пользователь – роль, модель отображения привилегия – роль и модель отображения роль – роль. Для упрощения логической структуры объектов управления вводится понятие иерархии ролей. Роль, входящая в иерархию, может включать другие роли, наследуя все привилегии включаемых ролей.

## 2 Теоретические основы безопасности в СУБД

### 2.1 Критерии защищенности БД

#### 2.1.1 Критерии оценки надежных компьютерных систем (TCSEC)

«Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название «Оранжевая книга», были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения. В данном документе были впервые нормативно определены такие понятия, как «политика безопасности», «ядро безопасности» (TCB) и т.д.

Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

В «Оранжевой книге» предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних – на качество самих средств защиты.

Рассмотрим эти требования подробнее:

##### 1. Политика безопасности

- **Политика безопасности** Система должна поддерживать точно определённую политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категоризированной информации (информации, отмеченной грифом секретности — типа «секретно», «сов. секретно» и т.д.).
- **Метки** С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

##### 2. Аудит

- **Идентификация и аутентификация** Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

- **Регистрация и учет** Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

### 3. Корректность

- **Контроль корректности** Средства защиты должны содержать независимые аппаратные и / или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.
- **Непрерывность защиты** Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

#### 2.1.2 Понятие политики безопасности

Согласно **GOST50922**: политика безопасности – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности (то есть как организация обрабатывает, защищает и распространяет информацию). Причём, политика безопасности относится к активным методам защиты, поскольку учитывает анализ возможных угроз и выбор адекватных мер противодействия.

#### 2.1.3 Совместное применение различных политик безопасности в рамках единой модели

Проблема совмещения различных политик безопасности возникает достаточно часто при администрировании компьютерных систем. Стандарты защиты информации в автоматизированных системах подразумевают наличие более одной политики разграничения доступа.

Так, в «Оранжевой книге» использование только дискреционного разделения доступа относит компьютерную систему к одному из классов безопасности группы «С», тогда как добавление мандатного контроля доступа позволяет претендовать на более высокий класс защищенности группы «В». Причем «Оранжевой книгой» подразумевается именно добавление мандатной политики безопасности (МПБ) с сохранением возможностей дискреционной политики безопасности (ДПБ).

В качестве еще одного примера совмещения политик безопасности можно привести системы управления базами данных, функционирующие на базе операционных систем семейства Windows. В системах управления базами данных наиболее распространенной является ролевая политика безопасности, но при этом данные хранятся в файлах, доступ к которым разграничивается операционной системой. В операционных системах базовой является ДПБ, но при этом реализуется на определенном уровне МПБ. Таким образом, требуется сопряжение трех различных политик безопасности.

#### **2.1.4 Интерпретация TCSEC для надежных СУБД (TDI)**

В дополнение к «Оранжевой книге» TCSEC, регламентирующей вопросы обеспечения безопасности в ОС, существуют аналогичный документ Национального центра компьютерной безопасности США для СУБД – TDI, («Пурпурная книга»).

#### **2.1.5 Оценка надежности СУБД как компоненты вычислительной системы**

##### **2.1.6 Монитор ссылок**

Контроль за выполнением субъектами (пользователями) определённых операций над объектами, путем проверки допустимости обращения (данного пользователя) к программам и данным разрешенному набору действий.

Обязательные качества для монитора обращений:

- Изолированность (неотслеживаемость работы)
- Полнота (невозможность обойти)
- Верифицируемость (возможность анализа и тестирования)

##### **2.1.7 Применение TCSEC к СУБД непосредственно**

##### **2.1.8 Элементы СУБД, к которым применяются TDI: метки, аудит, архитектура системы, спецификация, верификация, проектная документация**

Пурпурная книга

##### **2.1.9 Критерии безопасности ГТК**

ФСТЭКовская документация

## **2.2 Модели безопасности в СУБД**

Сегодня существует большое число различных теоретических моделей, которые позволяют описать практически все аспекты безопасности и обеспечивают средства защиты информации формально подтверждённой алгоритмической базой. Однако на практике воспользоваться результатами данных исследований не всегда удастся, потому что слишком часто теория защиты информации не согласуется с реальной жизнью. Дело в том, что теоретические исследования в области защиты информационных систем носит разрозненный характер и не составляет комплексной теории. Существующие технические разработки основаны на различных подходах проблеме, поэтому методы её

решения существенно различаются. Наибольшее развитие получили два подхода – это формальное моделирование политики безопасности и криптография. Эти различные по происхождению и решаемым задачам подходы взаимно дополняют друг друга. В отличие от криптографии, формальные модели безопасности предоставляют разработчикам защищенных систем принципы, которые лежат в основе архитектуры защищенной системы и определяют концепцию её построения.

Под *политикой безопасности* понимается совокупность норм и правил, определяющих меры по обеспечению безопасности данных, обрабатываемых в информационной системе. Для реализации политики безопасности, сформулированной в терминах естественного языка, необходимо представить ее формальное выражение. Его называют **модель политики безопасности** (или просто **модель безопасности**).

Далее мы разберем основные модели безопасности. Наиболее важные модели мы разберём подробно, а оставшиеся затронем кратко, отослав заинтересованного читателя к первоисточникам.

**Определения** Перед дальнейшим рассмотрением моделей безопасности сформулируем основные определения:

- Политика безопасности – совокупность норм и правил, определяющих меры по обеспечению безопасности данных, обрабатываемых в информационной системе.
- Модель безопасности – формальное выражение политики безопасности.
- Монитор безопасности – механизм реализации политики безопасности в автоматизированной системе, совокупность аппаратных, программных и специальных компонент системы, реализующих функции защиты и обеспечения безопасности (общепринятое сокращение – Trusted Computing Base, TCB).
- Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- Объект доступа – единица информационного ресурса, доступ к которой регламентируется правилами разграничения доступа.
- Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- Состояние системы – совокупность множеств субъектов, объектов и отношений между ними. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенными в модели критериями безопасности.

**Основная теорема безопасности (Basic Security Theorem)** Во время работы над моделью безопасности Белла-ЛаПадулы авторы пошли несколько дальше, и основываясь на формальном математическом аппарате, попытались строго доказать свойство защищенности своей модели. В результате они сформулировали и доказали "Основную теорему безопасности"(Basic Security Theorem):

Система безопасна тогда, и только тогда, когда ее начальное состояние безопасно, и любые переходы между ее состояниями также безопасны. Тогда и любое по-

следующее состояние этой системы также будет безопасным, вне зависимости от обрабатываемой информации и конкретных процессов ее обработки.

Теорема предполагает, что имеется возможность проверить безопасность начального состояния и всех возможных переходов состояний, чтобы доказать безопасность всей системы.

За моделью Белла-ЛаПадулы последовали другие модели управления доступом, создатели которых доказывали основную теорему безопасности и для них. Считалось, что доказательство этой теоремы доказывает безопасность и надежность самой модели.

Так продолжалось до середины 1980-х годов, когда Дж. Маклеан (J. McLean) подверг основную теорему безопасности критике. Маклеан предположил и обосновал, что она абсолютно бесполезна в силу своей тривиальности. Теорема никак не адресует собственно понятие безопасности, но демонстрирует общее свойство всех систем, допускающих формальное представление в виде конечного автомата с индуктивными переходами между последовательными состояниями. Безопасность же, скорее неформальное понятие.

После этого, попытки формального математического обоснования надежности и безопасности различных моделей управления доступом прекратились. Вопрос о возможности формализации и строгом математическом доказательстве свойства защищенности при обработке информации в вычислительной системе остается открытым до настоящего времени.

### 2.2.1 Аспекты исследования моделей безопасности

Основная цель создания и формального описания политики безопасности – это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Исследование моделей безопасности выполняется с разных сторон. Можно выделить следующие аспекты:

- Сущности системы – субъекты и объекты.
- Возможные связи между сущностями системы.
- Разрешенные функции перехода между состояниями системы.
- Выполнение основной теоремы безопасности.
- Реализация монитора безопасности.

### 2.2.2 Классификация моделей безопасности

Обычно говоря о моделях безопасности имеют ввиду модели разграничения доступа. Различают три основные модели контроля доступа:

1. **Дискреционная** (англ. discretionary access control, DAC);
2. **Мандатная** (англ. mandatory access control, MAC);
3. **Ролевая** (англ. role-based access control, RBAC).

### 2.2.3 Дискреционная модель

Политика дискреционного управления доступом реализована в большинстве защищенных информационных систем и исторически является первой проработанной в теоретическом и практическом плане. Первые описания моделей дискреционного доступа появились еще в 60-х годах и подробно представлены в литературе.

На практике дискреционная модель доступа предполагает, что для каждого объекта в системе определен субъект-владелец. Этот субъект может самостоятельно устанавливать необходимые, по его мнению, права доступа к любому из своих объектов для остальных субъектов, в том числе и для себя самого. Логически владелец объекта является владельцем информации, находящейся в этом объекте. При доступе некоторого субъекта к какому-либо объекту система контроля доступа лишь считывает установленные для объекта права доступа и сравнивает их с правами доступа субъекта. Кроме того, предполагается наличие в ОС некоторого выделенного субъекта – администратора дискреционного управления доступом, который имеет привилегию устанавливать дискреционные права доступа для любых, даже ему не принадлежащих объектов в системе.

Кратко рассмотрим основные модели безопасности.

**HRU** Модель безопасности Харрисона-Руззо-Ульмана (HRU-модель) (середина 1970-х гг.) реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа (**Zegzhda**). Названа в честь трёх его авторов: Майкла Харрисона, Уолтера Руззо и Джеффри Ульмана.

Главной особенностью является матрица доступа с полным описанием пользовательских прав к файлам. Изменения в эту матрицу вводятся с помощью специальных команд.

**Представления модели.** Введем некоторые обозначения:

- $S$  — множество субъектов;
- $O$  — множество объектов;
- $R = (r_1, r_2, \dots, r_n)$  — множество прав доступа.

Для реализации этих прав в данной модели используется матрица доступов  $M$ , строки которой соответствуют субъектам, а столбцы — объектам. На пересечении строчек и столбцов указаны права доступа  $R$ , которыми обладает данный субъект по отношению к данному объекту. Тогда текущее состояние системы  $Q$  можно однозначно записать в таком виде:  $Q = (S, O, M)$ . Также вводят множество возможных операций  $A = (a_1, a_2, \dots, a_k)$ .

**Критерий безопасности системы.** Для заданной системы исходное состояние  $Q_0 = (S_0, O_0, M_0)$  называется безопасным относительно права  $r$ , если не существует такой последовательности команд, которая изменила бы заданное начальное состояние системы так, что право  $r$  записалось бы в ячейку  $M[s;o]$ , в которой оно отсутствовало в начальном состоянии  $Q_0$  (**Zegzhda**). Если это условие не выполнено, то произошла утечка информации.

**Определение.** Монооперационная команда – команда, состоящая из не более чем одной элементарной операции (**Zegzhda**).

**Определение.** Монооперационная система – система, все команды которой являются монооперационными.



**Теорема.** Существует алгоритм, проверяющий на безопасность исходное состояние  $Q_0$  монооперационной системы на безопасность относительно права  $r$  (**WikiHRU**).

**Теорема.** Задача определения безопасности исходного состояния  $Q_0$  системы общего вида для данного права  $r$  является неразрешимой (**WikiHRU**).

Основным преимуществом модели над другими дискреционными является строгость критерия безопасности (**WikiHRU**).

**Take-Grant** Несмотря на недостатки дискреционных моделей безопасности, относительно простая реализация их на практике побудила исследователей к усовершенствованию моделей типа HRU, в которых проблема контроля распространения прав доступа алгоритмически не разрешима (**URFULecture10Models**).

Например, *система передачи прав доступа встраивается в систему разграничения в виде дополнительных прав*, образуя модель передачи прав доступа Take-Grant (1976). В этой модели доказывается безопасное состояние системы после изменения прав доступа к объекту или субъекту путем преобразования графов доступа (**URFULecture10Models**).

Модель представляет всю систему как направленный граф, где узлы — либо объекты, либо субъекты. Дуги между ними маркированы, и их значения указывают права, которые имеет объект или субъект (узел). В модели доминируют два правила: «брать» и «давать». Они играют в ней особую роль, переписывая правила, описывающие допустимые пути изменения графа (**WikiTakeGrant**). В общей сложности существует 4 правила преобразования:

- правило «брать»;
- правило «давать»;
- правило «создать»;
- правило «удалить».

Используя эти правила, можно воспроизвести состояния, в которых будет находиться система в зависимости от распределения и изменения прав доступа. Следовательно, можно проанализировать возможные угрозы для данной системы.

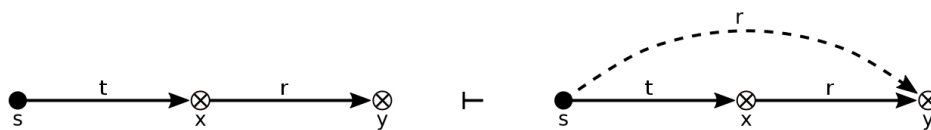
**Представления модели.** Введем некоторые обозначения:

- $S$  — множество субъектов;
- $O$  — множество объектов;
- $R = (r_1, r_2, \dots, r_n)$  — множество прав доступа.

**Правило «брать».**

Брать =  $\text{take}(r, x, y, s)$ ,  $r \in R$ . Пусть  $s \in S, x, y \in O$  — вершины графа  $G$ .

Тогда граф  $G$ :

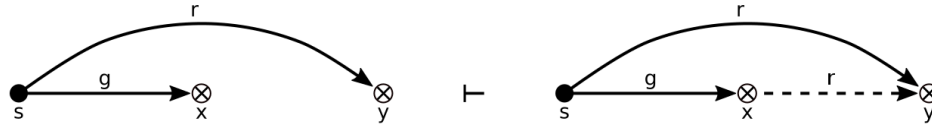


То есть субъект  $S$  берет у объекта  $X$  права  $r$  на объект  $Y$ .

### Правило «давать».

Давать =  $\text{grant}(r, x, y, s)$ ,  $r \in R$ . Пусть  $s \in S$ ,  $x, y \in O$  — вершины графа  $G$ .

Тогда граф  $G$ :



То есть субъект  $S$  дает объекту  $X$  права  $r$  на объект  $Y$ .

### Правило «создать».

Создать =  $\text{create}(p, x, s)$ ,  $r \in R$ . Пусть  $s \in S$ ,  $x, y \in O$  — вершины графа  $G$ .

Тогда граф  $G$ :

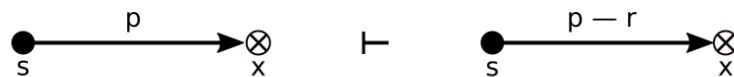


То есть субъект  $S$  берет  $r$ -доступный объект  $X$ .

### Правило «удалить».

Удалить =  $\text{remove}(r, x, s)$ ,  $r \in R$ . Пусть  $s \in S$ ,  $x, y \in O$  — вершины графа  $G$ .

Тогда граф  $G$ :



По-сути критерием безопасности системы при использовании модели Take-Grant является невозможность нарушения прав доступа при выполнении установленных правил.

Результатом модели становится представление системы как направленного графа с дугами - правами между субъектами и объектами.

Следующие две модели намного менее популярны, поэтому при их рассмотрении ссылаемся только на англоязычные источники.

**Action-Entity** Модель Acten (Action Entity) была предложена Буссолати и др. (**Jalili**) в 1983 г. Является расширением модели Take-Grant (**SecModels**):

- Дополнительные административные привилегии (использование, создание, удаление, ...)
- Предикаты авторизации – условия, которые должны быть выполнены для предоставления доступа
- Представление с использованием двух графиков (один для авторизации для статических действий и один для авторизации для динамических действий)

Цели расширения (**Jalili**):

- Исправление неизбирательности админских привилегий
- Увеличение контроля над транспортным потоком

*Каждый элемент системы, имеющий отношение к безопасности, рассматривается как **сущность (Entity)** (Jalili):*

- Сущность касается как субъектов, так и объектов
- Сущности – это типы ресурсов

*Выделяют два режима доступа – **действия (Action)** (Jalili):*

- статический;
- динамический.

**Статические действия (режим доступа).** Их выполнение не изменяет аутентификацию и состояние системы. Состоят из (**SecModels**):

- «Использование»: между пользователями, операторами и ресурсами ввода-вывода, приложениями, ...
- «Чтение»: для доступа к содержимому объекта
- «Написание» («Обновление»)
- «Создание»: сущностей
- «Удаление»: объекта

**Динамические действия (режим доступа).** Их выполнение изменяет аутентификацию и/или состояние системы. Состоят из (**SecModels**):

- «Грант» (предоставить, Grant): удержание субъектом  $E_i$  статического режима  $m$  по отношению к  $E_k$  позволяет  $E_i$  предоставить субъекту  $E_j$  режим  $m$  на  $E_k$
- «Отозвать»
- «Делегировать»: позволяет  $E_i$  предоставлять  $E_j$  динамическое разрешение на «грант», относящееся к режиму  $m$  на  $E_k$ . Авторизация для делегирования/отмены ограничена несколькими объектами
- «Отменить»

Вводится иерархия отношений между статическими режимами (**Jalili**):

- «Создание»/«Удаление» – 4
- «Обновление» – 3
- «Чтение» – 2

- «Использование» – 1

И между динамическими режимами (административными правами) (**Jalili**):

- «Делегировать»/«Отменить» – 2
- «Грант»/«Отозвать» – 1

В соответствии с этими иерархиями в модели Action Entity строят два графа:

- статических режимов;
- динамических режимов.

Вводят определённые правила для двух графов, которые являются критерием безопасности системы (**SecModels**). Подробное изложение можно найти в (**SecModels**) и в (**Jalili**).

**Wood** Единственным источником, где удалось найти хоть какую-то информацию о модели Woods является (**Jalili**). Согласно ему модель была разработана в 1979 г. Вудсом. Ориентация модели на управлении аутентификацией и контролем доступа в БД многоуровневой схемы. Модель рассматривает трехуровневую модель ANSI / SPARC, включая:

- Внешний уровень: ближайший к пользователю
- Концептуальный уровень: представление данных
- Внутренний уровень: ближайший к физическому хранению, не привязанный к аппаратным элементам.

Субъекты – пользователи системы:

- Авторизатор, который управляет авторизацией
- Пользователи, имеющие доступ к данным

Объекты – объекты концептуального уровня: каждый  $O$  принадлежит к категории типа, заданной функцией  $p(O)$ , указывает свою категорию типа ( $p(O)$ ):

- Категории типов на концептуальном уровне: набор сущностей, тип отношения и атрибут
- Атрибут может быть связан с одним набором объектов и сопоставляет набор объектов с набором значений
- Тип отношения – это двунаправленная ассоциация между двумя наборами сущностей и может иметь два имени

Состояние авторизации указывается в правилах доступа. Правила доступа имеют вид  $\langle s, o, t, p \rangle$ , где субъект  $s$  реализует режим доступа  $t$  к объекту  $o$  при условии  $p$ . Правила доступа определяются авторизатором. Основные правила указаны в концептуальном уровне, который представляет собой глобальное представление данных организации. Определение таблицы (на внешнем уровне) включает ограничения доступа, определяющие, какие типы доступа допустимы для каждый внешний объект  $e$  (каждая таблица и ее поля). Эти ограничения хранятся в ограничении доступа (Access Constraint, AC).

#### 2.2.4 Мандатная модель

Приведём классическое определение мандатной модели из *Оранжевой книги*.

Мандатная модель контроля доступа – это модель, в которой используются средства ограничения доступа к объектам, основанные на секретности информации, содержащейся в объектах, и обязательная авторизация действий субъектов для доступа к информации с присвоенным уровнем важности.

Важность информации определяется уровнем доступа, который приписывается всем объектам и субъектам. В сравнении с дискреционным мандатное управление доступом устанавливает гораздо более строгие правила определения прав доступа субъектов к объектам. Предполагается, что некоторый выделенный привилегированный субъект – администратор мандатного управления доступом – определяет необходимые, и согласованные с установленной в системе политикой безопасности, права доступа каждого из субъектов к каждому из объектов. Никакой другой субъект системы не может устанавливать или изменять свои, либо чьи-то еще права доступа к объектам. В такой системе права доступа пользователей определяются, прежде всего, интересами безопасности владельца всей системы.

Далее рассмотрим наиболее популярные мандатные модели безопасности.

**Модель Белла-ЛаПадулы** В середине 1970-х годов, два математика из MITRE Corporation – Д. Белл (D. Bell) и Л. ЛаПадула (L. LaPadula) – работая по проекту Министерства Обороны США, разработали мандатную модель, названную затем по их именам.

Основной задачей проекта была разработка и формальное обоснование модели управления доступом, функционально согласованную с методиками работы, принятым при обработке бумажной документации конфиденциального характера, т.е. имеющей грифы "секретно" "совершенно секретно" и т.п. Сложившаяся на тот момент практика обработки бумажной документации позволяла избежать несанкционированного доступа к информации, а также обладала приемлемой степенью удобства, поэтому было решено применить подобную схему и в вычислительной системе. Суть проекта состояла именно в этом. Интересно, что данный факт порой ускользает от внимания специалистов в области защиты информации.

Ниже дается упрощенное математическое описание модели Белла-ЛаПадулы.

Вычислительная система рассматривается в виде набора субъектов  $S_i$ , набора объектов  $O_j$  и матрицы управления доступом  $M[i * j]$ .

Имеется набор упорядоченных уровней секретности – иерархия уровней. Каждый субъект и каждый объект имеет назначенный ему *индивидуальный уровень секретности*. Кроме того, каждый субъект имеет еще *текущий уровень секретности*, который не может превосходить его индивидуальный уровень секретности. Таким образом, субъект может произвольно изменять свой текущий уровень секретности в диапазоне, не выше своего индивидуального уровня. Обычно используют четыре уровня секретности, каждый из которых доминирует над уровнем, находящимся ниже в иерархии: совершенно секретно (*top – secret*), секретно (*secret*), конфиденциально (*confidential*) и несекретно (*unclassified*). При этом верно следующее:  $top - secret \supset secret \supset confidential \supset unclassified$ .

Предполагается, что уровень секретности  $S_1$  доминирует над уровнем  $S_2$ , если он больше или равен  $S_2$ , т.е.  $S_1 \geq S_2$ .

Функция всех возможных в системе взаимных уровней секретностей субъектов и объектов  $F$  задается полным набором троек  $(f_S(S_i), S_i, f_O(O_j))$ . Здесь  $f_S(S_i)$  – индивидуальный уровень секретности субъекта  $S_i$ ,  $f_O(O_j)$  – индивидуальный уровень секретности объекта  $O_j$ , а  $f_C(S_i)$  – текущий уровень секретности субъекта  $S_i$ . Очевидно, что  $f_S(S_i)$  должен доминировать над  $f_C(S_i)$  для всех  $S_i$ . Рассматриваются четыре типа прав доступа субъекта к объекту:

1. **только чтение** (read-only, ro) произвольных участков данных;
2. **дополнение** (append, ad) - субъект может только записывать данные, размещая их в конце объекта;
3. **исполнение** (execute, ex) - субъект не может ни читать, ни записывать данные объекта, но может исполнять этот объект, как прикладную программу;
4. **чтение и запись** (read-write, rw) - субъект может и читать, и записывать данные объекта, по принципу произвольного доступа.

Набор всех типов прав доступа обозначают  $A$ , а любой его элемент –  $x$ .

Матрица управления доступом  $M[i; j]$  содержит в каждой из своих ячеек  $M_{ij}$  текущие дискреционные права доступа  $x$  (поднабор из  $A$ ) субъекта  $S_i$  к объекту  $O_j$ . Каждый столбец матрицы составляет атрибут управления объекта  $O_j$ , и является совокупным набором текущих прав доступа к нему всех субъектов. Атрибут управления для объекта  $O_j$  выдается субъекту  $S_k$  во время создания им этого объекта. Таким образом, субъект-создатель может устанавливать и отменять текущие дискреционные права доступа для любых субъектов, в том числе и для себя самого. Для этого он модифицирует соответствующие ячейки столбца  $M_j$  матрицы доступа  $M[i; j]$ , изменяя этим атрибут управления объекта  $O_j$ . Однако он не может передать право изменения атрибута управления какому-либо другому субъекту.

Всякое обращение субъекта  $S_i$  к объекту  $O_j$  с типом доступа  $x$  описывается тройкой  $(S_i, O_j, x)$ , а совокупность всех текущих обращений в системе – набором доступов  $b$ .

Теперь всю систему защиты можно описать в виде автомата конечных состояний с набором функций перехода между состояниями. Состояние модели  $z$  задается набором из четырех элементов  $(b, M[i; j], F, O_j)$ . С течением времени система принимает некоторую последовательность состояний  $z$ , с начальным состоянием  $z_0$ .

Разрешены следующие функции перехода между состояниями:

1. изменение набора текущих доступов  $b$ ;
2. изменение матрицы управления доступом  $M[i; j]$ ;
3. изменение набора объектов set  $O_j$ ;
4. субъект  $S_i$  может изменять свой текущий уровень секретности, но не выше его индивидуального уровня секретности.

Чтобы модель обеспечивала защиту, нужно чтобы всякий раз для функции перехода между состояниями удовлетворялся ряд дополнительных условий. Эти условия называется свойствами защиты. В модели Белла – ЛаПадулы устанавливаются и поддерживаются два мандатных и одно дискреционное свойства защиты<sup>10</sup>:

<sup>10</sup>В англоязычной литературе первое свойство называют simple security property, а второе – \*-property.

1. Субъект с определённым уровнем секретности не может иметь доступ на чтение объектов с более высоким уровнем секретности (англ. no read-up).
2. Субъект с определённым уровнем секретности не может иметь доступ на запись объектов с более низким уровнем секретности (англ. no write-down).
3. Использование матрицы доступа субъектов к объектам для описания дискреционного доступа.

Описанные три свойства защиты в обязательном порядке реализуются в системе защиты. Также требуется, чтобы каждое из свойств обязательно удовлетворялось для любого состояния системы защиты. Такие состояния называются безопасными состояниями.

Свойства защиты служат лишь общей директивой для действующих правил управления доступом. Текущий доступ  $(S_i, O_j, x)$  может быть предоставлен только в том случае, если выполнены следующие условия:

1. *ss – property*:  $f_C(S_i)$  доминирует над  $f_O(O_j)$ , если  $x = ro$  или  $x = rw$ .
2. *\* – property*:
  - 2.1  $f_O(O_j)$  доминирует над  $f_C(S_i)$ , если  $x = ad$ .
  - 2.2  $f_O(O_j)$  равен  $f_C(S_i)$ , если  $x = rw$ .
  - 2.3  $f_C(S_i)$  доминирует над  $f_O(O_j)$ , если  $x = ro$ .
3. *ds – property*:  $x$  находится в ячейке  $M_{ij}$  текущих прав доступа матрицы  $M[i * j]$ .

**Недостатки модели Белла-ЛаПадулы** Легко увидеть, что из описания модели Белла-ЛаПадулы нельзя определить формальных принципов назначения атрибутов безопасности субъектам и объектам. Действительно, в ней определены и обоснованы все правила управления доступом на основе атрибутов безопасности, но не способы их назначения при создании субъектов и объектов, импорте объектов в систему и т.д. Данный факт вызывает некоторые проблемы при практическом использовании модели.

Другим недостатком модели Белла-ЛаПадулы принято считать ее излишнюю строгость – возможность передачи информации только в сторону увеличения ее уровня секретности: "write up - read down". Это не всегда совместимо с нормальным функционированием реальной вычислительной системы. В силу тех же причин, несколько субъектов с разным уровнем секретности не могут равноправно получать доступ к одному объекту, например, совместно использовать один принтер для вывода информации на печать. Для устранения описанных ограничений в реальных системных обычно реализуют доверенных субъектов или доверенные программы, которые являются посредниками, гарантирующими безопасность несогласованных с моделью видов доступа.

Еще одним основанием для критики модели является проблема скрытых каналов (covert channels). Суть ее в том, что большинство ресурсов вычислительных систем, в том числе операционных систем UNIX - машинное время, устройства хранения информации - совместно и равноправно используются субъектами. Ресурсы выделяются субъектам по мере необходимости. Это рационально, однако также позволяет двум различным субъектам по предварительной договоренности произвольно обмениваться информацией без учета правил управления доступом, заложенных в модели защиты. Например, один из субъектов модулирует ресурсы системы, усиливая и уменьшая вычислительную

нагрузку на компьютер, или записывая и удаляя данные во внешней памяти. Это можно рассматривать как закодированную информацию, которую другой субъект считывает, измеряя периодически скорость выполнения своей задачи, или пытаясь также записать данные во внешнюю память.

Борьба со скрытыми каналами чрезвычайно трудна, так сами каналы являются следствием стремления к оптимальному использованию ресурсов системы. Обычно считается, что пропускная способность скрытых каналов слишком мала, и они не могут нанести серьезный ущерб безопасности. К тому же, они предполагают предварительный стговор двух субъектов, что маловероятно. Наличие скрытых каналов просто игнорируется, что можно в некоторой степени считать решением проблемы. В то же время, системы обработки особо конфиденциальной информации должны проектироваться с учетом проблемы скрытых каналов, возможно, в ущерб их производительности.

К числу недостатков модели Белла-ЛаПадулы также относят проблему целостности обрабатываемой информации, определяемую как невозможность искажения и/или уничтожения информации несанкционированными субъектами. Действительно, в рамках правил модели происходит передача информации в сторону повышения ее секретности. Однако разумно предположить, что менее секретная информация заслуживает меньшего доверия, равно как и менее секретный субъект, который может передать ее выше, исказив или уничтожив при этом конфиденциальные данные. Одновременно, с точки зрения системы, повышается (необоснованно) уровень доверия к передаваемой информации. То есть задача защиты информации в модели Белла-ЛаПадулы решается не полностью - конфиденциальная информация может быть искажена и даже уничтожена субъектом с низким уровнем секретности; хотя модель одновременно эффективно препятствует несанкционированному доступу к информации, ее утечке.

Целостность информации принято гарантировать реализацией в вычислительных системах специальных дополнительных моделей защиты. Дискреционное управление доступом также может обеспечить целостность информации в объекте, если его субъект-владелец позаботится об этом, установив соответствующие права доступа к нему.

Важно понимать, что сама по себе модель Белла-ЛаПадулы обладает рядом существенных недостатков, которые проявляются на практике. Тем не менее, она стала отправной точкой в области разработки мандатных моделей безопасности.

**Модель Биба** Модель Биба (англ., Biba model) оригинальным образом поддерживает целостность информации в системе, представимой в виде набора взаимодействующих субъектов и объектов. Она строится на основе иерархии уровней целостности (доверенности, достоверности) информации и двух основных правил ее обработки – аксиом целостности:

- аксиома простой целостности запрещает чтение информации более доверенным субъектом из менее достоверного объекта;
- аксиома целостности запрещает запись информации менее доверенным субъектом в более достоверный объект.

Таким образом, общие правила данной модели обозначить "no write up - no read down" что показывает ее логическую инверсию к модели Белла-ЛаПадулы.

Легко убедиться, что модель Биба позволяет решить проблемы поддержания целостности обрабатываемой информации и сохранения доверия к ней. Действительно, система запрещает произвольное повышение достоверности информации, более доверенные субъекты не могут пользоваться



менее достоверной информацией, а общий уровень достоверности комплексной информации, находящейся в объекте, равен минимальному уровню достоверности ее составляющих.

Как модель Белла-ЛаПадулы, так и модель Биба, часто называют моделями информационных потоков (information-flow model), так как информация в вычислительной системе может перемещаться при обработке только в виде потоков, разрешенных в рамках модели: "write up - read down"; "no write up - no read down".

Таким образом, единственной проблемой модели Белла-ЛаПадулы, к решению которой не существует общего подхода, является определение принципов назначения атрибутов безопасности субъектам и объектам.

**Модель Дион** Предлагается в качестве обязательной политики, которая одновременно обеспечивает секретность и целостность. Сочетает в себе принципы модели Биба (политика строгой последовательности). В модели нет дискреционной политики. Не позволяет передавать информацию от объектов к субъектам (через операции записи). Поток данных разрешен только между объектами, но никогда между объектами и субъектами. Содержит введение концепции связи между объектами для обмена информацией между ними.

Субъекты – это сущности, выполняемые в системе от имени пользователей. Каждому системному объекту назначается 3 уровня безопасности и 3 уровня целостности:

- ASL (Absolute Security Level) указывается при создании и фиксируется на всю жизнь предмета. Это второй уровень пользователя, соответствующий теме
- RSL (Read Security Level) – это самый высокий уровень безопасности, с которого субъекту разрешено читать
- WSL – это самый низкий уровень безопасности, на который субъекту разрешено писать
- AIL (Absolute Integrity Level) присваивается при создании и фиксируется на всю жизнь субъекта. Это уровень целостности пользователя, соответствующий предмету
- RIL: самый низкий уровень целостности, с которого субъекту разрешено читать
- WIL: наивысший уровень целостности, на который субъекту разрешено писать.

Устанавливаются ограничения – для каждого субъекта  $s$ :

$$\begin{aligned} WSL(s) &\leq ASL(s) \leq RSL(s) \\ RIL(s) &\leq AIL(s) \leq WIL(s) \end{aligned}$$

Субъект для которого строго соблюдается хотя бы одно неравенство удовлетворенный считается доверенным. Субъект может быть доверенным с точки зрения секретности, целостности или того и другого. Субъекты, для которых 4 отношения удовлетворяются знаком равенства, считаются недоверенными.

Объекты – любая сущность хранения данных в системе. Каждому объекту назначается 3 уровня безопасности и 3 уровня целостности:

- ASL (Absolute sec level) – уровень безопасности данных, содержащихся в объекте; фиксируется на весь срок службы объекта

- MSL (Migration sec level) – это самый высокий уровень безопасности, на который могут передаваться данные в объекте
- CSL (Corruption sec level) - это самый низкий уровень безопасности, с которого данные могут поступать в объект
- AIL (Absolute int level) - это уровень целостности данных в объекте
- MIL (Migration int level) - это самый низкий уровень целостности, на который могут передаваться данные в объекте
- CIL (Corruption int level) - это самый высокий уровень целостности, с которого данные могут поступать в объект

Аналогично:

$$CSL(o) \leq ASL(o) \leq MSL(o)$$

$$MIL(o) \leq AIL(o) \leq CIL(o)$$

В модели вводится ряд дополнительных аксиом и правил на отношения между субъектами и объектами.

**Многозначность в БД с многоуровневой секретностью** Как уже было показано, принципы модели безопасности Белла-ЛаПадулы сами по себе вполне здоровые, но на практике поддержание нескольких уровней защиты в пределах одной таблицы (или в одной базе данных) сопряжено с рядом серьезных проблем. Рассмотрим, например, следующую ситуацию.

Сотрудник военного ведомства, чьи персональные данные хранятся в базе данных с многоуровневой защитой, может иметь "настоящую" миссию, например быть сотрудником отдела по борьбе с терроризмом, и в то же время некоторое "прикрытие" согласно которому он является, допустим, членом отряда десантников. При этом в базе данных должна быть представлена и реальная информация, и прикрытие.

Мы могли бы расширить модель безопасности, добавив свойство секретности не только для каждой строки, но и на уровне элементов. Но это расширение приведет к новым серьезным проблемам, поскольку каждый элемент в строке может принимать одно из нескольких возможных значений, в зависимости от уровня доступа субъекта. Такое положение дел на фундаментальном уровне нарушает один из важнейших принципов реляционных баз данных – требование первой нормальной формы (1NF)<sup>11</sup>.

Решение проблемы поэлементной классификации основано на идее многозначности – когда в рамках одной таблицы может существовать множество записей с одним и тем же значением первичного ключа, но разными полями. Многозначность впервые была применена в 1988 г. в модели безопасной базы данных SeaView (Secure Data Views).

<sup>11</sup> Таблица считается приведенной к первой нормальной форме, если выполняются следующие условия:

- В таблице не должно быть дублирующих строк;
- В каждой ячейке таблицы должно храниться атомарное значение (одно не составное значение);
- В столбце должны храниться данные одного типа;
- Не должно быть массивов и списков.

**SeaView** Модель SeaView (secure data view) была предложена Дороти Деннингом в 1987 г. Она состоит из мандатной, дискреционной моделей, а также вспомогательной для добавления и классификации новой информации поступающей в базу данных. SeaView состоит из двух слоев:

- **MAC** обязательный контроль доступа. Этот уровень соответствует обязательной политике безопасности моделей Bell-LaPadula и Biba.
- **Trusted Computing Base (TCB)** определяет концепцию многоуровневых отношений, поддерживает дискреционные средства управления для многоуровневых отношений и представлений, а также формализует поддерживаемые политики. TCB построен поверх MAC.

Модель SeaView использует субъекты, объекты и классы доступа. Класс доступа состоит из:

- **Класс секретности** Класс секретности соответствует уровню безопасности модели Bell-LaPadулы
- **Класс целостности** Класс целостности соответствует уровню целостности модели Биба

Объекты MAC - это файлы, к которым должен быть предоставлен доступ. Субъекты MAC - это процессы, действующие от имени пользователей, и им назначается классификация этого пользователя. Каждому пользователю назначаются:

- Класс минимальной секретности (minsecrecy)
- Класс минимальной целостности (minintegrity)
- Классы секретности и целостности, первоначально назначенные пользователю, обозначаются maxsecrecy и maxintegrity

Каждому объекту назначаются классы:

- Класс для записи (minsecrecy, maxintegrity)
- Класс для чтения (maxsecrecy, minintegrity)

Причем для каждого объекта класс чтения должен быть выше класса записи. Субъект считается доверенным, если класс чтения строго больше класса записи.

**Jajodia&Sandhu** Модель Джаджодиа–Сандху является производной от модели SeaView. Она модифицирует алгоритм, который разлагает многоуровневое отношение на одноуровневые фрагменты, а также модифицирует алгоритм восстановления, который восстанавливает исходное многоуровневое отношение (**Osama**).

В модели Джаджодиа–Сандху алгоритм декомпозиции использует только горизонтальную фрагментацию, поскольку вертикальной фрагментации не требуется. Это приводит к улучшению алгоритма восстановления в модели Джаджодиа–Сандху по сравнению с алгоритмом восстановления в модели SeaView, поскольку можно восстановить многоуровневое отношение без необходимости выполнять операции соединения; для восстановления многоуровневого отношения требуются только операции объединения (**Osama**).

В модели Джаджодиа–Сандху есть две основные проблемы (**Osama**):

- Семантическая неоднозначность: предположим, что есть два кортежа в отношениях с уровнями безопасности  $U$  и  $S$ , и нет кортежа с уровнем безопасности  $TS$ . Если пользователю с уровнем безопасности  $TS$  необходимо получить информацию из отношения, он не может решить, какая информация является правильной, потому что значения из кортежа  $U$  и кортежа  $S$  в отношении будут извлечены в результате запроса
- Операционная неполнота: предположим, что существует два несравнимых уровня безопасности,  $M1$  и  $M2$ , наименьшая верхняя граница которых соответствует уровню безопасности  $S$ , а наибольшая нижняя граница – уровню безопасности  $U$ . Пользователь с уровнем безопасности  $S$  не может вставлять кортежи, которые содержат атрибуты с уровнями безопасности  $U$ ,  $M1$  и  $M2$

**Smith&Winslett** В модели Смита–Уинслетта многоуровневая реляционная база данных рассматривается как набор обычных реляционных баз данных, в которых все базы данных используют одну и ту же схему. Эта модель не поддерживает безопасность на уровне каждого отдельного атрибута. Уровень безопасности может быть назначен только атрибутам первичного ключа и кортежам в целом (**Osama**).

Многоуровневая реляционная схема задается как  $R(A_{pk}, C_{pk}, A_1, \dots, A_n, T_C)$ , где  $A_{pk}$  обозначается как атрибут данных первичного ключа,  $C_{pk}$  - атрибут классификации первичного ключа, который содержит уровень безопасности первичного ключа. Атрибут данных  $A_1 \dots A_n$  обозначается как атрибуты данных, а  $T_C$  обозначается как атрибут классификации кортежа, который содержит уровень безопасности кортежа (**Osama**).

Согласно этим правилам определяется доступ для обновления и чтения. Модификация базы данных (вставка, удаление и обновление) пользователем может изменить данные только на уровне безопасности пользователя. Запрос от пользователя с уровнем безопасности  $L$  может получить доступ к данным именно из тех баз данных, уровень которых не выше уровня  $L$  (**Osama**).

В этой модели была добавлена семантика, основанная на концепции веры. Модель Смита–Уинслетта также известна как модель семантики, основанная на убеждениях, а также представила концепцию базового кортежа. Базовый кортеж – это самый низкий уровень безопасности кортежа базы данных, в котором утверждается существование объекта. Таким образом, процедура обновления устраняет проблемы, присутствующие в модели Джаджодиа–Сандху, но ограничивает объем обновления одним объектом (**Osama**).

**Решеточная** Управление доступом на основе решеток (Lattice-Based Access Control, LBAC) - это сложная модель управления доступом, основанная на взаимодействии между любой комбинацией объектов (например, ресурсов, компьютеров и приложений) и субъектов (таких как отдельные лица, группы или организации) (**LBAC**).

В этом типе модели управления принудительным доступом на основе меток решетки используется для определения уровней безопасности, которые может иметь объект и к которым субъект может иметь доступ. Субъекту разрешен доступ к объекту только в том случае, если уровень безопасности субъекта больше или равен уровню безопасности объекта (**LBAC**).

Математически уровень безопасности доступа также может быть выражен в терминах решетки (набор частичного порядка), где каждый объект и субъект имеют наибольшую нижнюю границу (совпадение) и наименьшую верхнюю границу (соединение) прав доступа. Например, если двум

субъектам А и В требуется доступ к объекту, уровень безопасности определяется как соответствие уровней А и В. В другом примере, если два объекта X и Y объединены, они образуют другой объект Z, которому присваивается уровень безопасности, образованный объединением уровней X и Y (**LBAC**).

LBAC также известен как ограничение управления доступом на основе меток (или управление доступом на основе правил) в отличие от управления доступом на основе ролей (RBAC) (**LBAC**).

Модели управления доступом на основе решетки были впервые формально определены Деннингом (1976).

### 2.2.5 Ролевая модель

Ролевые модели безопасности нельзя отнести ни к дискреционным, ни к мандатным моделям, потому что управление доступом в них осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активации во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, основанный на компромиссе между гибкостью и простотой управления доступом (характерным для дискреционных моделей), так и жёсткостью правил контроля доступа (соответствующие мандатным моделям).

В ролевой модели классическое понятие *субъект* заменяется понятиями *пользователь* и *роль*. Пользователь – это человек, работающий с системой и выполняющий определённые обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логический связный набор полномочий, необходимый для осуществления определённой деятельности.

Такой подход в политике безопасности позволяет учесть разделение обязанностей и полномочий между участниками прикладного информационного процесса, так как с точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то какие полномочия ему необходимы для выполнения его служебных обязанностей (**Zegzhda**).

В качестве критерия безопасности ролевой модели используется следующее правило (**Zegzhda**): *система считается безопасной, если любой пользователь системы, работающий в определённом сеансе S, может осуществлять действия, требующие полномочия P только в том случае, если P принадлежит разрешениям S.*

### 2.2.6 Особенности реализации моделей безопасности в СУБД

Почти все крупные производители СУБД ограничиваются развитием концепции конфиденциальности, целостности и доступности данных, а их действия направлены, в основном, на преодоление существующих и уже известных уязвимостей, реализацию основных моделей доступа и рассмотрение вопросов, специфичных для конкретной СУБД. Такой подход обеспечивает решение конкретных задач, но не способствует появлению общей концепции безопасности для такого класса ПО, как СУБД. Это значительно усложняет задачу по обеспечению безопасности хранилищ данных на предприятии.

Обычно пользователей СУБД (субъектов) можно разделить на три группы, что влияет на применение определённых моделей безопасности (разграничения доступа) (**CitForumSafeDB**):

- Прикладные программисты – отвечают за создание программ, использующих базу данных. Программист может быть как пользователем, имеющим права создания и управления объектами (данными), так и пользователем, имеющим права только управления данными
- Конечные пользователи базы данных – работают с БД непосредственно через терминал или рабочую станцию. Как правило, конечные пользователи имеют строго ограниченный набор прав управления данными. Этот набор может определяться при конфигурировании интерфейса конечного пользователя и не изменяться. Политику безопасности в данном случае определяет администратор безопасности или администратор БД (если это одно и то же должностное лицо)
- Администраторы баз данных – образуют особую категорию пользователей СУБД. Они создают сами БД, осуществляют технический контроль функционирования СУБД, обеспечивают необходимое быстродействие системы. В обязанности администратора, также входит обеспечение пользователям доступа к необходимым им данным, написание (или оказание помощи в определении) необходимых пользователю внешних представлений данных. Администратор определяет политику безопасности

Отметим, что в настоящее время для контроля доступа в СУБД как правило используются дискреционные и ролевые модели. Мандатные модели значительно менее популярны в силу ряда недостатков в их использовании в СУБД.

**Дискреционные и ролевые модели доступа** При использовании дискреционных моделей в СУБД:

- Субъект – системный идентификатор, от имени которого СУБД выполняет определенные действия над определенными объектами. Понятие субъекта отличается от понятия пользователь компьютерной системы, поскольку инициировать изменение информации могут также и системные процессы
- Объект защиты – часть БД, на которую распространяется действие конкретного правила безопасности; это может быть группа отношений, отдельное отношение, подмножества атрибутов и т.д.
- Привилегия – действие над объектом защиты, которое может быть совершено от имени конкретного идентификатора (по сути элемент из множества отношений между субъектами и объектами – право на доступ)

Чаще всего владельцем базы данных является Администратор БД. Ему предоставлены все системные и объектные привилегии. В частности, он имеет право регистрации новых пользователей и предоставления им привилегий, как системных, так и объектных. Пользователь, имеющий системные привилегии, является владельцем всех созданных им объектов, имеет по отношению к ним все привилегии и может предоставлять их полностью или частично другим пользователям. Минимальной системной привилегией является право подключения к СУБД - привилегия входа (**Skakun**).

Пользователи могут быть объединены в специальные группы пользователей. Один пользователь может входить в несколько групп. Для пользователей с минимальным стандартным набором прав

вводится понятие группы PUBLIC. По умолчанию предполагается, что каждый вновь создаваемый пользователь, если специально не указано иное, относится к группе PUBLIC (как минимум в PostgreSQL).

Привилегии конкретному пользователю могут быть назначены администратором явно и неявно, например, через роль. Роль - это еще один возможный именованный носитель привилегий. Существует ряд стандартных ролей, которые проектируются при разработке СУБД. Также имеется возможность создавать новые роли, группируя в них произвольные полномочия. Введение ролей позволяет упростить управление привилегиями пользователей, структурировать этот процесс. Кроме того, введение ролей не связано с конкретными пользователями, поэтому роли могут быть определены и сконфигурированы до того, как определены пользователи системы.

**Операторы SQL предоставления и отмены привилегий.** В стандарте SQL определены два оператора GRANT и REVOKE для предоставления и отмены привилегий соответственно. *Оператор предоставления привилегий* имеет следующий формат (Skakun):

```
GRANT {<action list >|ALL PRIVILEGES} ON <object name>  
      TO {<user list >|PUBLIC} [WITH GRANT OPTION];
```

, где:

- <action list>(<список действий>) определяет набор действий из доступного списка действий над объектом данного типа (параметр ALL PRIVILEGES указывает, что разрешены все действия, допустимые для объектов данного типа),
- <object name>(<имя объекта>) определяет имя объекта защиты: таблицы, представления, хранимой процедуры или триггера,
- <user list>(<список пользователей>) определяет список идентификаторов пользователей, кому предоставляются данные привилегии. Вместо списка идентификаторов можно воспользоваться параметром PUBLIC.

Параметр WITH GRANT OPTION является необязательным и определяет режим, при котором передаются не только права на указанные действия, но и право передавать эти права другим пользователям. Передавать права в этом случае пользователь может только в рамках разрешенных ему действий. В общем случае набор привилегий зависит от реализации СУБД (определяется производителем). Выделяются привилегии манипулирования данными:

- SELECT — просматривать данные;
- INSERT [(<список полей>)] — добавлять данные;
- UPDATE [(<список полей >)] — обновлять данные;
- DELETE — удалять данные;
- REFERENCES [(<список полей >)] — ссылаться на указанные поля при определении ссылочной целостности;
- USAGE — использовать домены и ограничители целостности;
- EXECUTE — выполнять сохраненные процедуры и функции.

Среди привилегии создания/изменения объектов БД выделим наиболее часто используемые:

- CREATE <тип объекта> – создание объекта некоторого типа;
- ALTER <тип объекта> – изменение структуры объекта;
- DROP <тип объекта> – удаление объекта;
- ALL – все возможные действия над объектом.

Для отмены ранее назначенных привилегий в стандарте SQL определен оператор REVOKE. *Оператор отмены привилегий* имеет следующий синтаксис (**Skakun**):

```
REVOKE {<action list>|ALL PRIVILEGES} ON <object name>  
FROM {<user list>|PUBLIC} {CASCADE|RESTRICT};
```

Параметры CASCADE или RESTRICT определяют, каким образом должна производиться отмена привилегий. Параметр CASCADE отменяет привилегии не только пользователя, который непосредственно упоминался в операторе GRANT при предоставлении ему привилегий, но и всем пользователям, которым этот пользователь присвоил привилегии, воспользовавшись параметром WITH GRANT OPTION.

*Дискреционная модель является очень популярной у разработчиков СУБД. Она реализована в практически всех SQL-совместимых СУБД. Операторы SQL GRANT, REVOKE, DENY, реализующие дискреционную модель разграничения доступа, определены в стандарте языка SQL.*

**Ролевая модель в СУБД.** Рассмотренная дискреционная модель в СУБД очень похожа на ролевую модель. Основное отличие ролевой модели в СУБД – это обязательное использование принципа наименьших привилегий и то, что после авторизации пользователя в системе для него создается сессия. При реализации ролевой модели может быть введен ряд ограничений (**Skakun**): например, назначение роли главного администратора (суперпользователя) может быть предоставлено только одному пользователю, вводится запрет совмещения одним пользователем определенных ролей, ограничивается количество пользователей, одновременно выполняющих определенную роль и т.п.

К недостаткам ролевого разграничения доступа в СУБД относится отсутствие формальных доказательств безопасности компьютерной системы, возможность внесения дублирования и избыточности при предоставлении пользователям прав доступа и сложность конструирования ролей (**Skakun**).

Наряду с дискреционной, ролевая модель разграничения доступа, реализована во множестве развитых коммерческих СУБД, например: Microsoft SQL Server, Oracle, IBM DB2 (**Skakun**).

**Мандатные модели доступа в СУБД** Обычно мандатную модель доступа в СУБД реализуют с помощью модели Белл-ЛаПадула, о которой мы поговорим позже при рассмотрении конкретных примеров мандатных моделей.

Перечислим основные недостатки применения мандатных моделей доступа в СУБД (**Skakun**):

- Невозможность автоматизации назначения уровней секретности и определения границ защищаемых данных, что в больших системах может приводить к практически бесконечному ручному процессу конфигурации системы



- Снижение эффективности работы компьютерной системы, так как проверка прав доступа субъекта к объекту выполняется не только при открытии объекта в процессе субъекта, но и перед выполнением любой операции чтения из объекта или записи в объект
- Создание дополнительных неудобств в работе пользователей компьютерной системы, связанных с невозможностью изменения информации в неконфиденциальном объекте, если тот же самый процесс использует информацию из конфиденциального объекта (его уровень конфиденциальности больше нуля). Это зачастую решается путем разрешения пользователю выступать от имени субъекта с меньшим уровнем доступа, что в свою очередь приводит к деградации системы защиты.

*Из-за отмеченных недостатков мандатного разграничения доступа в реальных СУБД множество объектов, к которым применяется мандатное разграничение, является подмножеством множества объектов, доступ к которым осуществляется на основе дискреционного разграничения.*

Примером реализации мандатного подхода разграничения доступа можно считать компонент Oracle Label Security (OLS), реализованный в СУБД Oracle, начиная с 9 версии. Примером Российской СУБД, реализующей стандарт SQL-92 является СУБД ЛИНТЕР (Skakun).

**Проблемы реализации многозначности** Даже если отвлечься от проблемы хранения в базе данных разного рода легенд и прикрытий, многозначность все равно должна стать неотъемлемым свойством баз данных с многоуровневой защитой. Порассуждаем, каким образом следовало бы обрабатывать отношение с многоуровневой защитой в отсутствие многозначности. База данных может скрывать значения, недоступные пользователю или процессу по соображениям безопасности, и такое маскирование обычно осуществляется при помощи пустых значений (null values).

Напомним, что каждый кортеж существует в единственном экземпляре, поэтому непривилегированный процесс может попытаться записать неклассифицированные данные в столбцы кортежа, содержащие как бы пустые значения. В связи с этим в СУБД с многоуровневой защитой возникает проблема обработки таких операций, поскольку на самом деле значение столбца непустое, и замещать его нельзя. Естественно, что подобные попытки должны отвергаться средствами системы безопасности.

Однако неудача при выполнении операции модификации открывает определенные возможности, получившие название косвенных каналов (для получения закрытой информации), т. е. пути для снижения классификации данных (преднамеренного или случайного). Отказ в выполнении вроде бы вполне законной транзакции на модификацию пустых значений в базе данных с многоуровневой защитой выдает информацию о том, что эти элементы на самом деле не пусты, а содержат классифицированные данные. Уведомляя пользователя или процесс, не наделенных соответствующими полномочиями, о наличии скрытых данных в некотором кортеже, мы тем самым открываем косвенный канал.

Допустим, что СУБД с многоуровневой защитой симулирует выполнение подобных модификаций, чтобы не раскрывать скрытый канал. Если пользователь, только что изменивший некоторые данные, попытается обратиться к ним, ему ответят, что они отсутствуют. Тогда мы опять создаем косвенный канал.

А что если попытаться поддерживать в СУБД с многоуровневой защитой нечто вроде журнала

таких модификаций и использовать его для последующих выборок? Знакомая идея, и неудивительно – ведь мы только что говорили о многозначности. Даже если мы предусмотрим какое-нибудь специфическое решение для реализации многозначности, например хранить два экземпляра кортежей, – это всего лишь одна из реализаций. Важно, что многозначность – это существенное свойство данных с многоуровневой защитой, а как она будет реализована – это вопрос второстепенный, не имеющий отношения к самой идее по-разному представлять информацию для пользователей разных уровней благонадежности; хотя способы реализации многозначности остаются важным направлением для исследовательской работы.

Рассматривая проблему реализации многозначности, полезно обратить внимание на концептуальное сходство между многозначными кортежами в базе данных с многоуровневой защитой и кортежами с множественными значениями в хронологических базах данных. Напомним, что в большинстве реляционных баз данных с расширениями для поддержки хронологизма должны существовать несколько экземпляров одного кортежа с одним и тем же значением первичного ключа, чтобы обеспечить отображение и текущего состояния объекта, и исторической информации о нем. В реляционной СУБД с расширениями для поддержки многоуровневой защиты по существу присутствует такой же тип представления с той разницей, что определяющим признаком экземпляров некоторого кортежа в хронологической базе данных является время, а в базе данных с многоуровневой защитой – класс доступа. Хотя с других точек зрения, помимо реализации многозначности, хронологические СУБД и СУБД с многоуровневой защитой имеют мало общего, в связи с коммерциализацией СУБД обоих типов может оказаться полезным применять в них общие алгоритмы представления и доступа к многозначным кортежам.

Итак, многозначность, примененная впервые в проекте SeaView, стала общепринятой моделью реализации баз данных с многоуровневой защитой, в особенности реляционных. Многозначность активно исследуется и в качестве механизма обеспечения безопасности в объектно-ориентированных базах данных (развитие средств защиты в СУБД этого типа пока еще значительно отстает по сравнению с реляционными СУБД, но их значение будет неуклонно расти вместе со стремлением позиционировать ООСУБД на рынке продуктов для коммерческих и правительственных организаций).

## 3 Механизмы обеспечения целостности СУБД

### 3.1 Угрозы целостности СУБД

Задача обеспечения целостности предусматривает комплекс мер по предотвращению непреднамеренного изменения или уничтожения информации, используемой информационной системой управления или системой поддержки принятия решений. Изменение или уничтожение данных может быть следствием неблагоприятного стечения обстоятельств и состояния внешней среды (стихийные бедствия, пожары и т. п.), неадекватных действий пользователей (ошибки при вводе данных, ошибки операторов и т. п.) и проблем, возникающих при многопользовательской обработке данных (Lihonosov2011).

Например, с помощью SQL-операторов UPDATE, INSERT и DELETE можно изменить данные в СУБД. Опасность заключается в том, что пользователь, обладающий соответствующими привилегиями, может модифицировать все записи в таблице (Utebov2008).

## Основные виды и причины возникновения угроз целостности

Перечислим основные угрозы целостности информации (Pirogov2009):

1. **Отказ пользователей.** Под пользователями в данном случае мы понимаем широкий круг персонала, работающего с системой: операторы, программисты, администраторы и т. д.
  - Непреднамеренные ошибки. Непреднамеренная ошибка может вызвать непосредственно порчу данных или средств доступа, либо создать условия для реализации другой угрозы, например вторжения злоумышленника.
  - Нежелание работать с информационной системой. Причиной нежелания может, например, быть необходимость освоения новых возможностей системы или несоответствие системы запросам пользователей.
  - Невозможность работать с системой. Причиной невозможности работать с системой может быть как отсутствие соответствующей подготовки персонала, так и отсутствие необходимой документации по системе.
2. **Внутренние отказы информационной системы.** Основными источниками внутренних отказов могут быть:
  - случайное или умышленное отступление от правил эксплуатации. Например, правила могут предусматривать определенный набор параметров сервера (объем памяти, производительность процессора, объем дискового пространства, версия операционной системы и т. п.), на котором предполагается использовать ИС;
  - выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей;
  - ошибки конфигурирования системы. В сложных системах конфигурирование выполняется при установке и настройке системы. При неправильной настройке могут возникнуть проблемы в эксплуатации;
  - отказ программного обеспечения. Программное обеспечение может содержать ошибки, в том числе и такие, которые могут привести к серьезным повреждениям данных. Кроме этого преднамеренно может быть изменен алгоритм программы. Таким образом, следует защищать программное обеспечение информационной системы и от случайного повреждения, и от исправления непосредственно исполняемых модулей;
  - разрушение данных (возможно, преднамеренное). На заре компьютерной революции, когда не слишком заботились о безопасности данных, часто сталкивались с ситуацией, когда не совсем компетентный пользователь просто стирал важные (но плохо защищенные) данные с диска.
3. **Внешние источники возможного нарушения доступа к данным.** Данные источники могут быть вызваны и злонамеренными действиями людей, и стихийными бедствиями или авариями.
  - Отказ, повреждение или разрушение аппаратных средств (носителей информации, компьютеров, каналов связи). При интенсивном использовании отказ аппаратных средств случается совсем не редко, и меры безопасности должны учитывать такую возможность.

- Нарушение условий работы (системы связи, электропитание, отопление и т. п.). Отключение электричества совсем недавно было серьезной проблемой функционирования компьютерных систем. Источники бесперебойного питания должны защищать не только сами компьютеры, но все устройства в сети.
- Разрушение или повреждение помещений. Конечно, такая ситуация на первый взгляд кажется мало возможной, но это вполне вероятно в регионах, например, с сейсмической неустойчивостью.
- Невозможность или отказ обслуживающего персонала выполнять свои обязанности (стихийные бедствия, волнения, забастовка и т. п.). Отказ персонала выполнять свои обязанности для некоторых систем может привести к катастрофическим последствиям.
- Сетевые атаки, вирусные программы и другое вредоносное программное обеспечение. Сетевые атаки последнее время стали сильнейшим фактором риска информационных систем, работающих в Интернете.
- Разрушение информации намеренными действиями человека (диверсия). В данном случае речь идет о действиях людей, не являющихся обслуживающим персоналом данной системы.

### Способы противодействия

Основными средствами защиты целостности информации в ИС являются (Pirogov2009):

- транзакционные механизмы, позволяющие восстановить целостность данных в случае незначительных сбоев;
- контроль ввода данных. Много ошибок можно было бы избежать, если программы не пропускали бы заведомо противоречивые данные;
- использование средств защиты целостности СУБД;
- резервное копирование данных;
- периодическое тестирование системы на предмет нарушения целостности.

## 3.2 Метаданные и словарь данных

**Метаданные** – Это данные, описывающие другие данные. Это важный элемент хранилища данных, который предоставляет возможность показывать пользователю предметно-ориентированную структуру, а не набор абстрактно-связанных таблиц. Метаданные предназначены для хранения информации о происхождении данных, о любых изменениях данных, о расположении данных, об ограничениях на данные, о соответствии данных тем или иным объектам предметной области и т. д. (Pirogov2009)

## Назначение словаря данных

Согласно канонам реляционной модели данных описание структуры базы данных (описание объектов, входящих в базу данных) также должно храниться в таблицах. Такая структура называется словарем данных или системным каталогом. По сути, такие данные следует называть метаданными, т. е. данными, описывающими структуру других данных. В 1992 году в стандарте языка SQL было дано описание такого системного каталога. Но к этому времени в различных СУБД были приняты свои принципы хранения метаданных, отказаться от которых не так-то просто. В результате в одних СУБД вообще отсутствуют стандартные подходы к хранению метаданных, в других эти подходы в значительной степени дополнены своими особенностями. (Pirogov2009)

## Доступ к словарю данных

По 4 правилу Кодда (Dynamic On-Line Catalog Based on the Relational Model) словарь данных должен сохраняться в форме реляционных таблиц, и СУБД должна поддерживать доступ к нему при помощи стандартных языковых средств.

Для доступа к словарю данных используются инструкции SQL. Так как словарь данных доступен только для чтения, допускается выполнять только запросы таблиц и представлений. Можно запрашивать представления словаря, которые основаны на таблицах словаря, чтобы найти сведения, такие как (**Oracle**):

- определения всех объектов схемы в словаре (таблицы, представления, индексы, синонимы, последовательности, процедуры, функции, пакеты, триггеры и так далее);
- значения по умолчанию для столбцов;
- сведения об ограничениях целостности;
- имена пользователей Oracle;
- привилегии и роли, предоставленные каждому пользователю;
- другие общие сведения о базе данных.

## Состав словаря

В состав словаря данных базы данных входят *базовые таблицы* и *доступные пользователю представления*. Основу словаря данных составляет совокупность базовых таблиц, хранящих информацию о базе данных. Эти таблицы читаются и пишутся на системном уровне; они редко используются непосредственно пользователями. Словарь данных содержит доступные пользователю представления, которые суммируют и отображают в удобном формате информацию из базовых таблиц словаря. Эти представления декодируют информацию базовых таблиц, представляя ее в полезном виде, таком как имена пользователей или таблиц, и используют соединения и фразы WHERE, чтобы упростить информацию. Большинство пользователей имеют доступ к этим представлениям вместо базовых таблиц словаря. Словарь данных базы данных Oracle имеет два основных применения (Kirillov2009):

- Oracle обращается к словарю данных каждый раз, когда выдается предложение DDL;
- каждый пользователь Oracle может использовать словарь данных как только читаемый справочник по базе данных.

Словарь данных всегда доступен при открытой базе данных. Он размещается в табличном пространстве SYSTEM, которое всегда находится в состоянии online, когда база данных открыта.

### Представления словаря

Словарь данных состоит из нескольких наборов представлений. Во многих случаях такой набор состоит из трех представлений, содержащих аналогичную информацию и отличающихся друг от друга своими префиксами (Kirillov2009):

- USER — представление для пользователя;
- ALL — расширенное представление для пользователя;
- DBA — представление администратора.

Столбцы в каждом представлении набора идентичны, но имеются исключения. В представлениях с префиксом USER обычно нет столбца с именем OWNER (владелец); в представлениях USER под владельцем подразумевается пользователь, выдавший запрос. Некоторые представления DBA имеют дополнительные столбцы, которые содержат информацию, полезную для АБД.

#### Представления с префиксом USER:

- отражают окружение пользователя в базе данных, включая информацию о созданных им объектах, предоставленных им грантах и т. д.;
- выдают только строки, имеющие отношение к пользователю;
- имеют столбцы, идентичные с другими представлениями, с тем исключением, что столбец OWNER подразумевается (текущий пользователь);
- возвращают подмножество информации, предоставляемой представлениями ALL;
- могут иметь сокращенные общие синонимы для удобства.

**Представления с префиксом ALL** отражают общее представление о базе данных со стороны пользователя. Эти представления возвращают информацию об объектах, к которым пользователь имеет доступ через общие или явные гранты, помимо тех объектов, которыми владеет этот пользователь.

**Представления с префиксом DBA** показывают общее представление о базе данных, и предназначены для администраторов базы данных. Во время своей работы Oracle поддерживает набор "виртуальных" таблиц, в которых регистрируется текущая информация о базе данных. Эти таблицы называются динамическими таблицами производительности. Так как динамические таблицы

производительности не являются истинными таблицами, большинство пользователей не должно обращаться к ним. Динамические таблицы производительности принадлежат схеме SYS, а их имена начинаются с V\_\$. По этим таблицам создаются представления, а для представлений создаются синонимы, имена которых начинаются с V\$.

### 3.3 Понятие транзакции

Последовательность действий над данными, обрабатываемая СУБД как единая операция, будем называть **транзакцией**.

Из определения ясно, что транзакция может состоять из одной или нескольких команд языка SQL. При этом команды языка SQL могут перемежаться командами, не выполняющими непосредственно операций над данными (не читающими данные, не изменяющими данные, не изменяющими структуру данных). Таким образом, в качестве транзакции может быть выбрана любая часть программы, содержащая команды чтения или записи данных. В частности, транзакция может состоять всего из одной команды, например INSERT, или из сотен команд, изменяющих или не изменяющих данные. Понятие транзакции чрезвычайно емкое. Оно в действительности тесно связано с концептуальной моделью данных и всей информационной системы. Дело в том, что на уровне пользователя операции над данными носят предметный характер: начислить зарплату, уволить работника, перевести деньги на другой счет и т. п. Для выполнения таких операций часто необходимо выполнить десятки, и даже сотни команд языка SQL. Однако вся эта последовательность команд должна быть подчинена одной цели: операция уровня пользователя должна быть обязательно выполнена. Что будет, если при выполнении такой цепочки команд произойдет сбой? Как рассматривать тогда выполняемую операцию — как частично выполненную? Но как в дальнейшем система узнает, что операция была только частично выполнена, и как ее закончить? Все эти вопросы, в конце концов, и приводят к понятию **"транзакция"** (Pirogov2009).

#### Фиксация транзакции

Согласно требованиям ACID транзакция должна быть устойчивой. После своего завершения она сохраняется в системе, которую ничто не может вернуть в исходное (до начала транзакции) состояние, т. е. происходит фиксация транзакции, означающая, что ее действие постоянно даже при сбое системы. При этом подразумевается некая форма хранения информации в постоянной памяти как часть транзакции. При выполнении отдельных операций транзакции могут быть нарушены какие-либо требования целостности данных (в первую очередь имеются в виду корпоративные правила целостности, см. главу 2). Важно только то, что по окончании выполнения транзакции (фиксация транзакции) все правила целостности базы данных должны быть соблюдены. Согласно стандарту транзакция начинается с первой команды, которая обращается к данным. После этого транзакция продолжается до тех пор, пока не будет выполнена команда COMMIT WORK (или просто COMMIT) либо не будет закрыто соединение к базе данных. При выполнении команды COMMIT WORK происходит фиксация транзакции, другими словами, после этой команды откат транзакции уже будет невозможен (Pirogov2009).

#### Прокрутки вперед и назад

В результате сбоя СУБД могут возникнуть две потенциальные ситуации (Karpova2009):

- Блоки, содержащие подтверждённые модификации, не были записаны в файлы данных, так что эти изменения отражены лишь в журнале транзакций. Следовательно, журнал транзакций содержит подтверждённые данные, которые должны быть переписаны в файлы данных.
- Журнал транзакций и блоки данных содержат изменения, которые не были подтверждены. Изменения, внесенные неподтверждёнными транзакциями, во время восстановления БД должны быть удалены из файлов данных.

Для того чтобы разрешить эти ситуации, СУБД автоматически выполняет два этапа при восстановлении после сбоя: прокрутку вперед и прокрутку назад.

1. Прокрутка вперед заключается в применении к файлам данных всех изменений, зарегистрированных в журнале транзакций. После прокрутки вперед файлы данных содержат все как подтверждённые, так и неподтверждённые изменения, которые были зарегистрированы в журнале транзакций.
2. Прокрутка назад заключается в отмене всех изменений, которые не были подтверждены. Для этого используются журнал транзакций и сегменты отката, информация из которых позволяет определить и отменить те транзакции, которые не были подтверждены, хотя и попали на диск в файлы БД.

После выполнения этих этапов восстановления БД находится в согласованном состоянии и с ней можно работать.

### **Контрольная точка**

Критическим моментом в отказе системы является потеря содержимого основной (оперативной) памяти (в частности, буферов базы данных). Поскольку точное состояние любой выполнявшейся в момент отказа системы транзакции остается неизвестным, такая транзакция не может быть успешно завершена. Поэтому при перезапуске системы любая такая транзакция будет отменена (т.е. будет выполнен ее откат). Более того, при перезапуске системы, возможно, потребуется повторно выполнить некоторые транзакции, которые были успешно завершены до аварийного останова, но выполненные ими обновления еще не были перенесены из буферов оперативной памяти в физическую базу данных во вторичной памяти. Возникает очевидный вопрос: как система определяет в процессе перезапуска, какую транзакцию следует отменить, а какую выполнить повторно? Ответ заключается в том, что система автоматически создает контрольные точки с некоторым наперед заданным интервалом (обычно, когда в журнале накапливается определенное число записей). Для создания контрольной точки требуется, во-первых, выполнить принудительное сохранение содержимого буферов оперативной памяти в физической базе данных, и, во-вторых, осуществить принудительное сохранение специальной записи контрольной точки в журнале на физическом носителе. Запись контрольной точки содержит список всех транзакций, выполняемых в тот момент, когда создавалась контрольная точка (**Date2005**).

### **Откат**

Для управления транзакциями в системах, поддерживающих механизм транзакций и язык SQL, используется оператор отката транзакции (отмены изменений): **ROLLBACK [WORK]**. Для фиксации или отката транзакции система создаёт неявные точки фиксации и отката. По команде **rollback**



система откатит транзакцию на начало (на неявную точку отката). Для обеспечения целостности транзакции СУБД может откладывать запись изменений в БД до момента успешного выполнения всех операций, входящих в транзакцию, и получения команды подтверждения транзакции (commit). Но чаще используется другой подход: система записывает изменения в БД, не дожидаясь завершения транзакции, а старые значения данных сохраняет на время выполнения транзакции в сегментах отката. Сегмент отката (rollback segment, RBS) – это специальная область памяти на диске, в которую записывается информация обо всех текущих (незавершённых) изменениях. Обычно записывается "старое" и "новое" содержимое изменённых записей, чтобы можно было восстановить прежнее состояние БД при откате транзакции (по команде rollback) или при откате текущей операции (в случае возникновения ошибки). Данные в RBS хранятся до тех пор, пока транзакция, изменяющая эти данные, не будет завершена. Потом они могут быть перезаписаны данными более поздних транзакций. Команда savepoint запоминает промежуточную "текущую копию" состояния базы данных для того, чтобы при необходимости можно было вернуться к состоянию БД в точке сохранения: откатить работу от текущего момента до точки сохранения (rollback to <имя\_точки>) или зафиксировать работу от начала транзакции до точки сохранения (commit to <имя\_точки>). На одну транзакцию может быть несколько точек сохранения (ограничение на их количество зависит от СУБД). Для сохранения сведений о транзакциях СУБД ведёт журнал транзакций. Журнал транзакций — это часть БД, в которую поступают данные обо всех изменениях всех объектов БД. Журнал недоступен пользователям СУБД и поддерживается особо тщательно (иногда ведутся две копии журнала, хранимые на разных физических носителях). Форма записи в журнал изменений зависит от СУБД. Но обычно там фиксируется следующее:

- номер транзакции (номера присваиваются автоматически по возрастанию);
- состояние транзакции (завершена фиксацией или откатом, не завершена, находится в состоянии ожидания);
- точки сохранения (явные и неявные);
- команды, составляющие транзакцию, и проч.

Начало транзакции соответствует появлению первого исполняемого SQL-оператора. При этом в журнале появляется запись об этой транзакции (Karpova2009).

### **Транзакции как средство изолированности пользователей**

Поддержание механизма транзакций — показатель уровня развитости СУБД и основа обеспечения целостности базы данных. Транзакции также составляют основу изолированности в многопользовательских системах, где с одной базой данных параллельно могут работать несколько пользователей и (или) прикладных программ. Одна из основных задач СУБД — обеспечение изолированности, т. е. создание такого режима функционирования, при котором каждому пользователю казалось бы, что база данных доступна только ему. Такую задачу СУБД принято называть параллелизмом транзакций. Большинство выполняемых действий производится в теле транзакций. По умолчанию каждая команда выполняется как самостоятельная транзакция. Как было показано ранее, при необходимости пользователь может явно указать ее начало и конец, чтобы иметь возможность включить в нее несколько команд. Решение проблемы параллельной обработки базы данных

заключается в том, что строки таблиц блокируются, а последующие транзакции, модифицирующие эти строки, отвергаются и переводятся в режим ожидания. В связи со свойством сохранения целостности базы данных транзакции являются подходящими единицами изолированности пользователей. Действительно, если каждый сеанс взаимодействия с базой данных реализуется транзакцией, то пользователь начинает с того, что обращается к согласованному состоянию базы данных — состоянию, в котором она могла бы находиться, даже если бы пользователь работал с ней в одиночку. Если бы в СУБД не были реализованы механизмы блокирования, то при одновременном чтении и изменении одних и тех же данных несколькими пользователями могли бы возникнуть следующие проблемы одновременного доступа:

- проблема последнего изменения возникает, когда несколько пользователей изменяют одну и ту же строку, основываясь на ее начальном значении; тогда часть данных будет потеряна, т. е. каждая последующая транзакция перезапишет изменения, сделанные предыдущей. Выход из этой ситуации заключается в последовательном внесении изменений;
- проблема "грязного" чтения возможна в том случае, если пользователь выполняет сложные операции обработки данных, требующие множественного изменения данных перед тем, как они обретут логически верное состояние. Если во время изменения данных другой пользователь будет считывать их, то может оказаться, что он получит логически неверную информацию. Для исключения подобных проблем необходимо производить считывание данных после окончания всех изменений;
- проблема неповторяемого чтения является следствием неоднократного считывания транзакцией одних и тех же данных. Во время выполнения первой транзакции другая может внести в данные изменения, поэтому при повторном чтении первая транзакция получит уже иной набор данных, что приведет к нарушению их целостности или логической несогласованности;
- проблема чтения фантомов появляется после того, как одна транзакция выбирает данные из таблицы, а другая вставляет или удаляет строки до завершения первой. Выбранные из таблицы значения будут некорректны.

## **Сериализация транзакций**

Для того, чтобы добиться изолированности транзакций, в СУБД должны использоваться какие-либо методы регулирования совместного выполнения транзакций.

План (способ) выполнения набора транзакций называется сериальным, если результат совместного выполнения транзакций эквивалентен результату некоторого последовательного выполнения этих же транзакций.

Сериализация транзакций – это механизм их выполнения по некоторому сериальному плану. Обеспечение такого механизма является основной функцией компонента СУБД, ответственного за управление транзакциями. Система, в которой поддерживается сериализация транзакций, обеспечивает реальную изолированность пользователей.

Основная реализационная проблема состоит в выборе метода сериализации набора транзакций, который не слишком ограничивал бы их параллельность. Приходящим на ум тривиальным

решением является действительно последовательное выполнение транзакций. Но существуют ситуации, в которых можно выполнять операторы разных транзакций в любом порядке с сохранением сериальности. Примерами могут служить только читающие транзакции, а также транзакции, не конфликтующие по доступу к объектам базы данных.

Между транзакциями могут существовать следующие виды конфликтов:

- W-W - транзакция 2 пытается изменить объект, измененный не закончившейся транзакцией 1;
- R-W - транзакция 2 пытается изменить объект, прочитанный не закончившейся транзакцией 1;
- W-R - транзакция 2 пытается читать объект, измененный не закончившейся транзакцией 1.

Практические методы сериализации транзакций основываются на учете этих конфликтов (**Serial**).

### Методы сериализации транзакций

Существуют два базовых подхода к сериализации транзакций – основанный на синхронизационных захватах объектов базы данных и на использовании временных меток. Суть обоих подходов состоит в обнаружении конфликтов транзакций и их устранении. Предварительно заметим, что для каждого из подходов имеются две разновидности – пессимистическая и оптимистическая. При применении пессимистических методов, ориентированных на ситуации, когда конфликты возникают часто, конфликты распознаются и разрешаются немедленно при их возникновении. Оптимистические методы основываются на том, что результаты всех операций модификации базы данных сохраняются в рабочей памяти транзакций. Реальная модификация базы данных производится только на стадии фиксации транзакции. Тогда же проверяется, не возникают ли конфликты с другими транзакциями.

Пессимистические методы сравнительно просто трансформируются в свои оптимистические варианты (**Serial**).

## 3.4 Блокировки

Блокировки, называемые также синхронизационными захватами объектов, могут быть применены к разному типу объектов. Наибольшим объектом блокировки может быть вся БД, однако этот вид блокировки делает БД недоступной для всех приложений, которые работают с данной БД. Следующий тип объекта блокировки — это таблицы. Транзакция, которая работает с таблицей, блокирует ее на все время выполнения транзакции. Этот вид блокировки предпочтительнее предыдущего, потому что позволяет параллельно выполнять транзакции, которые работают с другими таблицами.

В ряде СУБД реализована блокировка на уровне страниц. В этом случае СУБД блокирует только отдельные страницы на диске, когда транзакция обращается к ним. Этот вид блокировки еще более мягок и позволяет разным транзакциям работать даже с одной и той же таблицей, если они обращаются к разным страницам данных.

В некоторых СУБД возможна блокировка на уровне строк, однако такой механизм блокировки требует дополнительных затрат на поддержку этого вида блокировки.

В настоящее время проблема блокировок является предметом большого числа исследований (Intuit).

### Режимы блокировок

Рассматривают два типа блокировок (синхронизационных захватов) (Intuit):

- совместный режим блокировки — нежесткая, или разделяемая, блокировка, обозначаемая как S (Shared). Этот режим обозначает разделяемый захват объекта и требуется для выполнения операции чтения объекта. Объекты, заблокированные таким образом, не изменяются в ходе выполнения транзакции и доступны другим транзакциям также, но только в режиме чтения;
- монопольный режим блокировки — жесткая, или эксклюзивная, блокировка, обозначаемая как X (eXclusive). Данный режим блокировки предполагает монопольный захват объекта и требуется для выполнения операций занесения, удаления и модификации. Объекты, заблокированные данным типом блокировки, фактически остаются в монопольном режиме обработки и недоступны для других транзакций до момента окончания работы данной транзакции.

### Правила согласования блокировок

Захваты объектов несколькими транзакциями по чтению совместимы, то есть нескольким транзакциям допускается читать один и тот же объект, захват объекта одной транзакцией по чтению не совместим с захватом другой транзакцией того же объекта по записи, и захваты одного объекта разными транзакциями по записи не совместимы. В примере, представленном на рис. 1 считается, что первой блокирует объект транзакция А, а потом пытается получить к нему доступ транзакция В.

		Транзакция В		
		Разблокирована	Нежесткая блокировка	Жесткая блокировка
Транзакция А	Разблокирована	Да	Да	Да
	Нежесткая блокировка	Да	Да	Нет
	Жесткая блокировка	Да	Нет	Нет

Рис. 1: Правила применения жесткой и нежесткой блокировок транзакций

### Двухфазный протокол синхронизационных блокировок

В базах данных и обработке транзакций двухфазная блокировка (2PL) — это метод управления параллелизмом, который гарантирует сериализуемость. Это также имя результирующего набора графиков транзакций базы данных (истории). Протокол использует блокировки, применяемые

транзакцией к данным, которые могут блокировать (интерпретировать как сигналы для остановки) другие транзакции от доступа к тем же данным в течение жизни транзакции.

По протоколу 2PL блокировки (locks) применяются и удаляются в два этапа:

1. Фаза расширения: блокировки берутся и ни одна блокировка не освобождается.
2. Фаза сокращения: блокировки освобождаются и ни одна блокировка не берётся.

В базовом протоколе используются два типа блокировок: Shared и Exclusive locks. Уточнения базового протокола могут использовать больше типов блокировок. Используя блокировки, блокирующие процессы, 2PL могут подвергаться взаимоблокировкам, которые являются результатом взаимной блокировки двух или более транзакций (**Wiki**).

### Тупиковые ситуации, их распознавание и разрушение

Одним из наиболее чувствительных недостатков метода сериализации транзакций на основе синхронизационных захватов является возможность возникновения тупиков (deadlocks) между транзакциями.

Вот простой пример возникновения тупика между транзакциями T1 и T2:

1. транзакции T1 и T2 установили монополярные захваты объектов r1 и r2 соответственно;
2. после этого T1 требуется совместный захват r2, а T2 - совместный захват r1;
3. ни одна из транзакций не может продолжаться, следовательно, монополярные захваты не будут сняты, а совместные - не будут удовлетворены.

Поскольку тупики возможны, и никакого естественного выхода из тупиковой ситуации не существует, то эти ситуации необходимо обнаруживать и искусственно устранять.

Основой обнаружения тупиковых ситуаций является построение (или постоянное поддержание) графа ожидания транзакций. Граф ожидания транзакций - это ориентированный двудольный граф, в котором существует два типа вершин - вершины, соответствующие транзакциям, и вершины, соответствующие объектам захвата. В этом графе существует дуга, ведущая из вершины-транзакции к вершине-объекту, если для этой транзакции существует удовлетворенный захват объекта. В графе существует дуга из вершины-объекта к вершине-транзакции, если транзакция ожидает удовлетворения захвата объекта.

Легко показать, что в системе существует ситуация тупика, если в графе ожидания транзакций имеется хотя бы один цикл.

Для распознавания тупика периодически производится построение графа ожидания транзакций (как уже отмечалось, иногда граф ожидания поддерживается постоянно), и в этом графе ищутся циклы. Традиционной техникой (для которой существует множество разновидностей) нахождения циклов в ориентированном графе является редукция графа.

Не вдаваясь в детали, редукция состоит в том, что прежде всего из графа ожидания удаляются все дуги, исходящие из вершин-транзакций, в которые не входят дуги из вершин-объектов. (Это как бы соответствует той ситуации, что транзакции, не ожидающие удовлетворения захватов, успешно завершились и освободили захваты). Для тех вершин-объектов, для которых не осталось входящих дуг, но существуют исходящие, ориентация исходящих дуг изменяется на противоположную (это

моделирует удовлетворение захватов). После этого снова срабатывает первый шаг и так до тех пор, пока на первом шаге не прекратится удаление дуг. Если в графе остались дуги, то они обязательно образуют цикл.

Предположим, что нам удалось найти цикл в графе ожидания транзакций. Что делать теперь? Нужно каким-то образом обеспечить возможность продолжения работы хотя бы для части транзакций, попавших в тупик. Разрушение тупика начинается с выбора в цикле транзакций так называемой транзакции-жертвы, т.е. транзакции, которой решено пожертвовать, чтобы обеспечить возможность продолжения работы других транзакций.

Грубо говоря, критерием выбора является стоимость транзакции; жертвой выбирается самая дешевая транзакция. Стоимость транзакции определяется на основе многофакторная оценка, в которую с разными весами входят время выполнения, число накопленных захватов, приоритет.

После выбора транзакции-жертвы выполняется откат этой транзакции, который может носить полный или частичный характер. При этом, естественно, освобождаются захваты и может быть продолжено выполнение других транзакций.

Естественно, такое насильственное устранение тупиковых ситуаций является нарушением принципа изолированности пользователей, которого невозможно избежать.

Заметим, что в централизованных системах стоимость построения графа ожидания сравнительно невелика, но она становится слишком большой в по-настоящему распределенных СУБД, в которых транзакции могут выполняться в разных узлах сети. Поэтому в таких системах обычно используются другие методы сериализации транзакций.

Еще одно замечание. Чтобы минимизировать число конфликтов между транзакциями, в некоторых СУБД (например, в Oracle) используется следующее развитие подхода. Монопольный захват объекта блокирует только изменяющие транзакции. После выполнении операции модификации предыдущая версия объекта остается доступной для чтения в других транзакциях. Кратковременная блокировка чтения требуется только на период фиксации изменяющей транзакции, когда обновленные объекты становятся текущими (**Serial**)

### 3.5 Ссылочная целостность

Ссылочная целостность. Ссылочная целостность относится непосредственно к связям между таблицами. Если кратко, то ссылочная целостность должна отвечать на вопрос: что будет со строками одной таблицы, если в связанной таблице выполняется какая-либо операция модификации? Для того чтобы понять логику ссылочной целостности, будем считать таблицу главной в паре связанных таблиц, если она содержит первичный ключ, с помощью которого осуществляется связь. Вторую таблицу будем считать подчиненной таблицей. Теперь выделим три вида операции над связанными таблицами: удаление из главной таблицы, обновление строк главной таблицы, вставка в подчиненную таблицу.

1. Удаление строк из главной таблицы. Если удаляемая строка не связана со строками другой таблицы, то удалять можно без всяких последствий. Но если удаляемая строка связана со строками другой таблицы, то надо подумать, что же будет с этими строками. Просто оставить их без изменения нельзя, т. к. не понятно, как быть со значениями внешних ключей. В принципе, возможны следующие четыре сценария, поддерживаемые основными СУБД:

- строки из подчиненной таблицы должны быть удалены вместе со связанными строками из подчиненной таблицы. Такой механизм называется каскадированием;
  - если удаляемая строка из главной таблицы связана со строками из подчиненной таблицы, то такая операция удаления должна быть отвергнута. Данный механизм наиболее безопасен и предпочтителен при построении информационной системы;
  - если строка в подчиненной таблице связана с удаляемой строкой в главной таблице, то внешнему ключу следует присвоить значение NULL;
  - если строка в подчиненной таблице связана с удаляемой строкой в главной таблице, то внешнему ключу следует присвоить значение, принятое по умолчанию.
2. Обновление строк из главной таблицы. Если обновляемая строка не связана со строками другой таблицы или обновляются столбцы, не относящиеся к первичному ключу, то обновлять можно без всяких последствий. Но если обновляемая строка связана со строками другой таблицы и обновляется первичный ключ, то здесь, как и в предыдущем случае, возможны четыре сценария:
- первичные ключи из главной таблицы обновляются вместе с внешними ключами подчиненной таблицы. Как и в случае с подобной операцией удаления, этот механизм называется каскадированием;
  - если обновляемая строка связана с какой-либо строкой подчиненной таблицы, то операция обновления должна быть отвергнута;
  - если строка в подчиненной таблице связана с обновляемой строкой в главной таблице, то внешнему ключу следует присвоить значение NULL;
  - если строка в подчиненной таблице связана с обновляемой строкой в главной таблице, то внешнему ключу следует присвоить значение, принятое по умолчанию.
3. Вставка строк в подчиненную таблицу. Здесь возможны следующие механизмы.
- Строка в подчиненной таблице вставляется вместе со строкой в главной таблице. Здесь важно иметь в виду, что в главной таблице для всех столбцов должны быть определены значения по умолчанию. Последовательность добавления такая: вначале добавляется строка в главную таблицу и определяется значение первичного ключа. Затем добавляется строка в подчиненную таблицу, в которой значению внешнего ключа присваивается значение первичного ключа в главной таблице.
  - Строка в подчиненную таблицу добавляется только при условии, что соответствующая ей строка в главной таблице уже существует.
  - При добавлении строки в подчиненную таблицу внешнему ключу присваивается значение NULL.
  - При добавлении строки в подчиненную таблицу внешнему ключу присваивается значение по умолчанию.

В некоторых простых СУБД отсутствует возможность устанавливать связи между таблицами и, таким образом, поддерживать ссылочную целостность. В этом случае поддержание ссылочной целостности полностью ложится на плечи программиста. Другими словами, связь между таблицами должна быть реализована на уровне прикладного программного обеспечения.

## Декларативная и процедурная ссылочные целостности

Различают два способа реализации ограничений целостности:

- Декларативная поддержка ограничений целостности.
- Процедурная поддержка ограничений целостности.

**Декларативная поддержка ограничений целостности** заключается в определении ограничений средствами языка определения данных (DDL - Data Definition Language). Обычно средства декларативной поддержки целостности (если они имеются в СУБД) определяют ограничения на значения доменов и атрибутов, целостность сущностей (потенциальные ключи отношений) и ссылочную целостность (целостность внешних ключей). Декларативные ограничения целостности можно использовать при создании и модификации таблиц средствами языка DDL или в виде отдельных утверждений (ASSERTION).

Например, следующий оператор создает таблицу PERSON и определяет для нее некоторые ограничения целостности:

```
CREATE TABLE PERSON
(Pers_Id INTEGER PRIMARY KEY,
Pers_Name CHAR(30) NOT NULL,
Dept_Id REFERENCES DEPART(Dept_Id) ON UPDATE CASCADE ON DELETE CASCADE);
```

После выполнения оператора для таблицы PERSON будут объявлены следующие ограничения целостности:

- Поле Pers\_Id образует потенциальный ключ отношения.
- Поле Pers\_Name не может содержать null-значений.
- Поле Dept\_Id является внешней ссылкой на родительскую таблицу DEPART, причем, при изменении или удалении строки в родительской таблице каскадно должны быть внесены соответствующие изменения в дочернюю таблицу.

**Процедурная поддержка ограничений целостности** заключается в использовании триггеров и хранимых процедур.

Не все ограничения целостности можно реализовать декларативно. Примером такого ограничения может служить требование из примера 1, утверждающее, что поле Dept\_Kol таблицы DEPART должно содержать количество сотрудников, реально числящихся в подразделении. Для реализации этого ограничения необходимо создать триггер, запускающийся при вставке, модификации и удалении записей в таблице PERSON, который корректно изменяет значение поля Dept\_Kol. Например, при вставке в таблицу PERSON новой строки, триггер увеличивает на единицу значение поля Dept\_Kol, а при удалении строки - уменьшает. Заметим, что при модификации записей в таблице PERSON могут потребоваться даже более сложные действия. Действительно, модификация записи в таблице PERSON может заключаться в том, что мы переводим сотрудника из одного отдела в другой, меняя значение в поле Dept\_Id. При этом необходимо в старом подразделении уменьшить количество сотрудников, а в новом - увеличить (**TransCit**).



## Внешний ключ

**Внешний ключ** – это ограничение целостности, в соответствии с которым множество значений внешнего ключа является подмножеством значений первичного или уникального ключа родительской таблицы (Karpova2009).

Ограничение целостности по внешнему ключу проверяется в двух случаях (Karpova2009):

- при добавлении записи в подчинённую таблицу СУБД проверяет, что в родительской таблице есть запись с таким же значением первичного ключа;
- при удалении записи из родительской таблицы СУБД проверяет, что в подчинённой таблице нет записей с таким же значением внешнего ключа.

### Способы поддержания ссылочной целостности

СУБД имеют механизм автоматического поддержания ссылочной целостности. Любая операция, изменяющая данные в таблице, вызывает автоматическую проверку ссылочной целостности. При этом (WikiLink):

- При операции добавления записи автоматически проверяется, ссылаются ли внешние ключи в этой записи на существующие записи в заявленных при описании связанных таблиц. Если выясняется, что операция приведёт к появлению некорректных ссылок, она не выполняется — система возвращает ошибку.
- При операции редактирования записи проверяется:
  - если изменяется её первичный ключ и на данную запись имеются ссылки, то операция редактирования завершается с ошибкой;
  - если изменяется какой-то из внешних ключей, хранящихся в этой записи, и после изменения внешний ключ будет ссылаться на несуществующую запись, то операция редактирования завершается с ошибкой.
- При операции удаления записи проверяется, нет ли на неё ссылок. Если ссылки имеются, то возможно три варианта дальнейших действий (фактически выполняемый зависит от СУБД и от выбора программиста, который он должен сделать при описании связи):
  - Запрет — удаление блокируется и возвращается ошибка.
  - Каскадное удаление — в одной транзакции производится удаление данной записи и всех записей, ссылающихся на данную. Если на удаляемые записи также есть ссылки и настройки также требуют удаления, то каскадное удаление продолжается дальше. Таким образом, после удаления данной записи в базе не остаётся ни одной записи, прямо или косвенно ссылающейся на неё. Если хотя бы одну из ссылающихся записей удалить не получается (либо для неё настроен запрет, либо происходит какая-либо ещё ошибка), то все удаления запрещаются.
  - Присвоение NULL — во все внешние ключи записей, ссылающихся на данную, записывается маркер NULL. Если хотя бы для одной из ссылающихся записей это невозможно (например, если поле внешнего ключа описано как NOT NULL), то удаление запрещается.

### 3.6 Правила(триггеры)

Триггеры являются одной из разновидностей хранимых процедур. Их исполнение происходит при выполнении для таблицы какого-либо оператора языка манипулирования данными (DML). Триггеры используются для проверки целостности данных, а также для отката транзакций.

Триггер представляет собой специальный тип хранимых процедур, запускаемых сервером автоматически при попытке изменения данных в таблицах, с которыми триггеры связаны. Каждый триггер привязывается к конкретной таблице. Все производимые им модификации данных рассматриваются как одна транзакция. В случае обнаружения ошибки или нарушения целостности данных происходит откат этой транзакции. Тем самым внесение изменений запрещается. Отменяются также все изменения, уже сделанные триггером.

Триггер представляет собой весьма полезное и в то же время опасное средство. Так, при неправильной логике его работы можно легко уничтожить целую базу данных, поэтому триггеры необходимо очень тщательно отлаживать.

В отличие от обычной подпрограммы, триггер выполняется неявно в каждом случае возникновения триггерного события, к тому же он не имеет аргументов. Приведение его в действие иногда называют запуском триггера (**IntuitTrigg**)

#### Цели использования правил

С помощью триггеров достигаются следующие цели (**IntuitTrigg**):

- проверка корректности введенных данных и выполнение сложных ограничений целостности данных, которые трудно, если вообще возможно, поддерживать с помощью ограничений целостности, установленных для таблицы;
- выдача предупреждений, напоминающих о необходимости выполнения некоторых действий при обновлении таблицы, реализованном определенным образом;
- накопление аудиторской информации посредством фиксации сведений о внесенных изменениях и тех лицах, которые их выполнили;
- поддержка репликации.

#### Способы задания, моменты выполнения

Создает триггер только владелец базы данных. Это ограничение позволяет избежать случайного изменения структуры таблиц, способов связи с ними других объектов и т.п. Основной формат команды CREATE TRIGGER показан ниже:

```
<Определение_триггера> ::=  
CREATE TRIGGER имя_триггера  
BEFORE | AFTER <триггерное_событие>  
ON <имя_таблицы>  
[REFERENCING  
  <список_старых_или_новых_псевдонимов>]
```

```
[FOR EACH { ROW | STATEMENT}]  
[WHEN(условие_триггера)]  
<тело_триггера>
```

Триггерные события состоят из вставки, удаления и обновления строк в таблице. В последнем случае для триггерного события можно указать конкретные имена столбцов таблицы.

Триггер – это процедура БД, которая привязана к конкретной таблице и вызывается автоматически при наступлении определённого события (добавления, удаления или модификации данных этой таблицы).

В отличие от обычной подпрограммы, триггер выполняется неявно в каждом случае возникновения триггерного события, к тому же он не имеет аргументов. Приведение его в действие иногда называют запуском триггера.

Время запуска триггера определяется с помощью ключевых слов BEFORE ( триггер запускается до выполнения связанных с ним событий) или AFTER (после их выполнения).

Выполняемые триггером действия задаются для каждой строки ( FOR EACH ROW ), охваченной данным событием, или только один раз для каждого события ( FOR EACH STATEMENT ).

Обозначение <список\_старых\_или\_новых\_псевдонимов> относится к таким компонентам, как старая или новая строка ( OLD / NEW ) либо старая или новая таблица ( OLD TABLE / NEW TABLE ). Ясно, что старые значения не применимы для событий вставки, а новые – для событий удаления (**IntuitTrigg**).

### 3.7 События

#### Назначение механизма событий

Механизм событий в базе данных (database events) позволяет прикладным программам и серверу базы данных уведомлять другие программы о наступлении в базе данных определенного события и тем самым синхронизировать их работу (**OSP**).

#### Сигнализаторы событий. Типы уведомлений о происхождении события. Компоненты механизма событий

Операторы языка SQL, обеспечивающие уведомление, часто называют сигнализаторами событий в базе данных (database event alerters). Функции управления событиями целиком ложатся на сервер базы данных.

Механизм событий используется следующим образом. Вначале в базе данных для каждого события создается флажок, состояние которого будет оповещать прикладные программы о том, что некоторое событие имело место (оператор CREATE DBEVENT - СОЗДАТЬ СОБЫТИЕ). Далее во все прикладные программы, на ход выполнения которых может повлиять это событие, включается оператор REGISTER DBEVENT (ЗАРЕГИСТРИРОВАТЬ СОБЫТИЕ), который оповещает сервер базы данных, что данная программа заинтересована в получении сообщения о наступлении события. Теперь любая прикладная программа или процедура базы данных может вызвать событие оператором RAISE DBEVENT (ВЫЗВАТЬ СОБЫТИЕ). Как только событие произошло, каждая зарегистрированная программа может получить его, для чего должна запросить очередное

сообщение из очереди событий (оператор GET DBEVENT - ПОЛУЧИТЬ СОБЫТИЕ) и запросить информацию о событии, в частности, его имя (оператор SQL INQUIRE\_SQL) (OSP).

## 4 Механизмы обеспечения конфиденциальности в СУБД

### 4.1 Классификация угроз конфиденциальности СУБД

#### 4.1.1 Причины, виды, основные методы нарушения конфиденциальности

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Основными причинами нарушения конфиденциальности информации являются: - несоблюдение персоналом норм, требований, правил эксплуатации АС; - ошибки в проектировании АС и систем защиты АС; - ведение противостоящей стороной технической и агентурной разведок.

Источник: [http://www.o-salo.narod.ru/page4.htm#\\_Toc287060195](http://www.o-salo.narod.ru/page4.htm#_Toc287060195)

Угрозы конфиденциальности информации направлены на несанкционированное перемещение информации от носителя-источника к носителю-получателю (угроза разглашения, утечки, несанкционированного доступа). Уязвимость информации к преднамеренным действиям злоумышленников или иных заинтересованных лиц является наиболее опасной. Как уже отмечалось выше, различные виды уязвимости обусловлены угрозами разглашения, НСД Уязвимость информации к разглашению – несанкционированному сообщению защищаемой информации лицам, не имеющим

Уязвимость информации к НСД – противоправному преднамеренному овладению защищаемой информацией лицом, не имеющим права доступа к ней, – определяется наличием у информации, ее носителя или у самой системы защиты недостатков, которые создают возможность получения информации, ее модификации, уничтожения, блокирования доступа к ней.

Уязвимость информации к утечке – неконтролируемому распространению защищаемой информации за пределы круга лиц, которым эта информация была доверена, – возникает, как и в случае разглашения, из-за неправильной организации работы с информацией, а также в связи с "дырами" в системе защиты информации, неосторожными или умышленными действиями людей, допущенных к работе с защищаемыми сведениями. Утечка может происходить по акустическому, визуально-оптическому, материально-вещественному и электромагнитному каналам. Следовательно, уязвимость информации к утечке определяется слабыми сторонами носителя информации, среды, окружающей информацию, и технических средств, находящихся в непосредственной близости от носителей информации.

Источник: <https://bit.ly/2XLDyia>

Также, угрозы делят на умышленные и неумышленные (баги в ПО, сгнили провода и тп), умышленные в свою очередь делят на активные и пассивные:

Активные угрозы имеют целью нарушение нормального функционирования ИТ посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

Раскрытие конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы информационной технологии или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Умышленные угрозы подразделяются также на следующие виды:

Внутренние - возникают внутри управляемой организации. Они чаще всего сопровождаются социальной напряженностью и тяжелым моральным климатом на экономическом объекте, который провоцирует специалистов выполнять какие-либо правонарушения по отношению к информационным ресурсам

Внешние - Пассивные угрозы направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование ИТ

Далее приведены некоторые угрозы ИБ:

**Раскрытие конфиденциальной информации** - это неконтролируемый выход конфиденциальной информации за пределы информационной технологии или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Раскрытие конфиденциальной информации может быть следствием:

- разглашения конфиденциальной информации
- утечки информации по различным, главным образом техническим, каналам (по визуальнo-оптическим, акустическим, электромагнитным и др
- несанкционированного доступа к конфиденциальной информации различными способами

**Несанкционированный доступ к информации** выражается в противоправном преднамеренном овладении конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей
- применение подслушивающих устройств (закладок)
- дистанционное фотографирование
- перехват акустических излучений и восстановление текста принтера
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов
- копирование носителей информации с преодолением мер защиты
- маскировка под зарегистрированного пользователя ("маскарад")
- использование недостатков языков программирования и операционных систем

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки - это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет

взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации - канал несанкционированного доступа.

**Несанкционированное использование информационных ресурсов**, с одной стороны, является последствиями ее утечки и средством ее компрометации. С другой стороны, оно имеет самостоятельное значение, так как может нанести большой ущерб управляемой системе (вплоть до полного выхода информационной технологии из строя) или ее абонентам.

**Незаконное использование привилегий.** Любая защищенная технология содержит средства, используемые в чрезвычайных ситуациях, или средства, которые способны функционировать с нарушением существующей политики безопасности. Например, на случай внезапной проверки пользователь должен иметь возможность доступа ко всем наборам системы. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции. Большинство систем защиты в таких случаях используют наборы привилегий, т. е. для выполнения определенной функции требуется определенная привилегия. Обычно пользователи имеют минимальный набор привилегий, администраторы - максимальный. Наборы привилегий охраняются системой защиты. Несанкционированный (незаконный) захват привилегий возможен при наличии ошибок в системе защиты, но чаще всего происходит в процессе управления системой защиты, в частности, при небрежном пользовании привилегиями.

**"Взлом системы"** - умышленное проникновение в информационную технологию, когда взломщик не имеет санкционированных параметров для входа. Способы взлома могут быть различными, и при некоторых из них происходит совпадение с ранее описанными угрозами. Например, использование пароля пользователя информационной технологии, который может быть вскрыт, например, путем перебора возможных паролей.

Источник: <https://www.intuit.ru/studies/courses/3609/851/lecture/31660>

#### 4.1.2 Типы утечки конфиденциальной информации из СУБД, частичное разглашение

Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной. Утечка информации возможна по разным причинам.

Умышленные утечки:

Инсайдеры и избыточные права. К этому виду относятся случаи, основной причиной которых стали действия сотрудников, имеющих доступ к секретам легально, в силу своих служебных обязанностей. Все варианты инсайда условно можно разделить на две группы: в одном случае сотрудник, не имея доступа к информации, получает ее незаконно, а в другом он обладает официальным доступом к закрытым данным и умышленно выносит их за пределы компании.

Кража информации (извне). Проникновение в компьютер с помощью вредоносных программ и похищение информации с целью использования в корыстных интересах. На хакерские атаки приходится 15% от всего объема утечек информации. Вторжение в устройство извне и незаметная установка вредоносных программ позволяют хакерам полностью контролировать систему и получать доступ к закрытым сведениям, вплоть до паролей к банковским счетам и картам. Для этого могут применяться различные программы вроде «тройанских коней». Главный атрибут данного вида утечки — активные действия внешних лиц с целью доступа к информации.

Взлом программного обеспечения. Приложения, используемые в рабочем процессе или на личном компьютере сотрудника, часто имеют незакрытые уязвимости, которые можно эксплуатировать и получать тем самым различные небезопасные возможности вроде исполнения произвольного кода или повышения привилегий.

Вредоносные программы (бэкдоры, трояны) нацелены на причинение вреда владельцу устройства, позволяют незаметно проникать в систему и затем искажать или полностью удалять информацию, подменять ее другими, похожими данными.

Кражи носителей. Весьма распространенный вариант утечек, который случается в результате преднамеренного хищения устройств с информацией — ноутбуков, смартфонов, планшетов и других съемных носителей данных в виде флешек, жестких дисков.

Случайные утечки. К этому виду можно отнести инциденты, которые происходят из-за потери носителей данных (флешек, ноутбуков, смартфонов) или ошибочных действий сотрудников организации. Результатом может быть размещение конфиденциальной информации в интернете. Также не последнюю роль играет человеческий фактор, когда сотрудник по недосмотру открывает доступ к закрытым данным всем желающим.

Источник: <https://www.anti-malware.ru/threats/leaks>

#### **4.1.3 Соотношение защищенности и доступности данных**

??? В. Г. Проскурин. Защита в операционных системах 2014.pdf с 7 п4 мб об этом Суть такая, слишком жесткие политики безопасности могут повлечь нарушение доступности. Пример: запретить поль-лю SYSTEM в WINDOWS доступ к исполняемым файлам - тогда ОС нормально загрузиться не сможет.

#### **4.1.4 Получение несанкционированного доступа к конфиденциальной информации путем логических выводов**

Нередко путем логического вывода можно извлечь из базы данных информацию, на получение которой стандартными средствами у пользователя не хватает привилегий.

Если для реализации контроля доступа используются представления и эти представления допускают модификацию,

Основным средством борьбы с подобными угрозами, помимо тщательного проектирования модели данных, является механизм размножения строк. Суть его в том, что в состав первичного ключа, явно или неявно, включается метка безопасности, за счет чего появляется возможность хранить в таблице несколько экземпляров строк с одинаковыми значениями "содержательных" ключевых полей. Наиболее естественно размножение строк реализуется СУБД, поддерживающих метки безопасности (например, в INGRES/ Enhanced Security), однако и стандартными SQL-средствами можно получить удовлетворительное решение.

Рассмотрим базу данных, состоящую из одной таблицы с двумя столбцами - имя пациента и диагноз. Предполагается, что имя является первичным ключом. Каждая из строк таблицы относится к одному из двух уровней секретности - высокому (HIGH) и низкому (LOW). Соответственно, и пользователи подразделяются на два уровня благонадежности, которые мы также будем называть высоким и низким. К высокому уровню секретности относятся сведения о пациентах, находящихся под надзором правоохранительных органов или страдающих специфическими заболеваниями.

На низком уровне располагаются данные о прочих пациентах, а также информация о некоторых "секретных" пациентах с "маскировочным" диагнозом. Части таблицы могут выглядеть примерно так:

Имя	Диагноз
Иванов	СПИД
Петров	Сифилис
Сидоров	Стреляная рана

Таблица 4.

Данные с высоким уровнем секретности.

Имя	Диагноз
Иванов	Пневмония
Ивлев	Рак легких
Ярцев	Ожог второй степени
Суворов	Микроинфаркт

Таблица 5.

Данные с низким уровнем секретности.

Обратим внимание на то, что сведения о пациенте по фамилии Иванов присутствуют на обоих уровнях, но содержат разные диагнозы.

Мы хотим реализовать такую дисциплину доступа, чтобы пользователи с низким уровнем благонадежности могли манипулировать только данными на своем уровне и не имели возможности сделать какие-либо выводы о присутствии в секретной половине сведений о конкретных пациентах. Пользователи с высоким уровнем благонадежности должны иметь доступ к секретной половине таблицы, а также к информации о прочих пациентах. Дезинформирующих строк о секретных пациентах они видеть не должны:



Имя	Диагноз
Иванов	СПИД
Ивлев	Рак легких
Петров	Сифилис
Сидоров	Стреляная рана
Ярцев	Ожог второй степени
Суворов	Микроинфаркт

Таблица 6.

Данные, доступные пользователю с высоким уровнем секретности (обратим внимание, что строка "Иванов Пневмания" здесь отсутствует.).

#### 4.1.5 Методы противодействия. Особенности применения криптографических методов

В целях обеспечения конфиденциальности информации используются следующие криптографические примитивы:

- Симметричные криптосистемы
- Асимметричные криптосистемы

В симметричных криптосистемах для зашифрования и расшифрования информации используется один и тот же общий секретный ключ, которым взаимодействующие стороны предварительно обмениваются по некоторому защищённому каналу. Также к симметричным системам относят те, в которых получение ключа расшифрования из ключа шифрования является тривиальной операцией. В зависимости от объёма данных, обрабатываемых за одну операцию шифрования, симметричные шифры делятся на блочные, в которых за одну операцию шифрования происходит преобразование одного блока данных (32 бита, 64, 128 или больше), и потоковые, в которых работают с каждым символом открытого текста по отдельности (например, с 1 битом или 1 байтом). Использование блочного шифра подразумевает разделение открытого текста на блоки одинаковой длины, к каждому из которых применяется функция шифрования. Кроме того, результат шифрования следующего блока может зависеть от предыдущего. Данная возможность регулируется режимом работы блочного шифра. В качестве примеров симметричных криптосистем можно привести международные стандарты DES и пришедший ему на смену AES, оба являются Блочными. Пример потокового - RC4, который также может выступать в качестве генератора псевдослучайной последовательности случайных чисел.

Асимметричные криптосистемы характерны тем, что в них используются различные ключи для зашифрования и расшифрования информации, при этом получение ключа расшифрования из ключа шифрования вычислительно сложно. Ключ для зашифрования (открытый ключ) можно сделать общедоступным, с тем чтобы любой желающий мог зашифровать сообщение для некоторого получателя. Получатель же, являясь единственным обладателем ключа для расшифрования (секретный ключ), будет единственным, кто сможет расшифровать зашифрованные для него сообщения. Все используемые на сегодняшний день асимметричные криптосистемы работают с открытым текстом, составляющим несколько сотен или тысяч бит, поэтому классификация таких систем по объёму обрабатываемых за одну операцию данных не производится. Примеры асимметричных криптосистем

– RSA и схема Эль-Гамала.

Симметричные и асимметричные криптосистемы, а также различные их комбинации используются в АС прежде всего для шифрования данных на различных носителях и для шифрования трафика.

Источник: Криптографические методы защиты информации. Учебное пособие. Владимиров С. М., Габидулин Э. М., Колыбельников А. И., Кшевецкий А. С.

#### **4.1.6 Применение шифрования в базах данных**

Шифрование базы данных — использование технологии шифрования для преобразования информации, хранящейся в базе данных (БД), в шифротекст, что делает её прочтение невозможным для лиц, не обладающих ключами шифрования.

Основные подходы можно классифицировать по тому, на каком уровне происходит шифрование:

- Шифрование на уровне хранилища.
- Шифрование на уровне базы данных.
- Шифрование на уровне приложения.

##### **Шифрование на уровне хранилища:**

Также называемое «прозрачным» (Transparent Database Encryption, TDE). Данная технология, применяется, например, в продуктах Microsoft и Oracle для шифрования и дешифрования ввода-вывода файлов БД. Данные шифруются перед записью на диск и дешифруются во время чтения в память, что решает проблему защиты «неактивных» данных, но не обеспечивает сохранность информации при передаче по каналам связи или во время использования. Преимуществом TDE является то, что шифрование и дешифрование выполняются прозрачно для приложений, то есть их модификация не требуется.

##### **Реализация шифрование на уровне хранилища Microsoft:**

TDE применяется для файлов БД и журнала транзакций на уровне страниц. Страницы шифруются с помощью специального симметричного ключа шифрования базы данных (англ. Database Encryption Key), защищённого сертификатом, который хранится в БД master и шифруется её главным ключом, или асимметричным ключом, защищённым модулем расширенного управления ключами (англ. Extensible Key Manager, EKM). Применение TDE не увеличивает размер зашифрованной БД, а влияние на производительность незначительно.

##### **Реализация шифрование на уровне хранилища Oracle:**

TDE применяется для файлов БД на уровне столбцов. Для таблицы, содержащей выбранные к шифрованию столбцы, создаётся симметричный ключ шифрования, защищённый главным ключом, который хранится в безопасном месте за пределами БД, называемом бумажником (англ. Wallet). Зашифрованные ключи таблиц содержатся в словаре данных (англ. Data Dictionary).

##### **Шифрование на уровне базы данных:**

Одним из примеров шифрования на уровне базы данных является шифрование на уровне столбцов (Column-Level Encryption), которое записывает в базу данных уже зашифрованные данные, а саму базу данных — без дальнейшего шифрования — в хранилище. Особенностью шифрования на уровне столбцов является использование единого ключа при обработке данных одного столбца.

Ключи могут быть назначены пользователям и защищены паролем для предотвращения автоматической расшифровки, однако это усложняет администрирование БД. При использовании шифрования на уровне столбцов необходимо внесение изменений в клиентские приложения. Помимо этого уменьшается производительность БД.

#### **Шифрование на уровне приложений:**

В шифровании на уровне приложений процесс шифрования осуществляется приложением, которое создаёт или изменяет данные, то есть он происходит перед записью в базу данных. Этот подход является более гибким, так как приложению известны роли или права доступа пользователей, а также информация о том, какие данные являются конфиденциальными.

#### **Преимущества шифрования на уровне приложений:**

Одним из главных преимуществ шифрования, встроенного в приложение, является то, что нет необходимости использовать дополнительное решение для защиты данных при передаче по каналам связи, так как они отправляются уже зашифрованными. Ещё один плюс такого метода — это то, что кража конфиденциальной информации становится сложнее, так как злоумышленник должен иметь доступ к приложению для того, чтобы расшифровать данные, хранящиеся в БД.

#### **Недостатки шифрования на уровне приложений:**

Для реализации шифрования на уровне приложений необходимо внесение изменений не только в само приложение, но и в базу данных. Также могут возникнуть проблемы с производительностью БД, у которой, например, пропадает возможность индексирования и поиска. Ещё одним минусом является управление ключами в системе с таким шифрованием. Так как несколько приложений могут использовать БД, то ключи хранятся во многих местах, поэтому неправильное управление ими может привести к краже информации или невозможности её использования. В добавление к этому, если возникает необходимость изменения ключа, то для начала потребуется расшифровать все данные со старым ключом, и потом снова зашифровать, используя новый ключ.

## **4.2 Средства идентификации и аутентификации**

### **4.2.1 Общие сведения**

Начнем с понятий идентификации и аутентификации:

Идентификация объекта – это установление эквивалентности между объектом и его априорным обозначением (определением, представлением, образом, комплексом характеристик). Другими словами, идентификация это выделение объекта и установление для него отличительного набора параметров или характеристик. Например для идентификации пользователя это наличие идентифицирующей его информации, на основе которой можно однозначно

Аутентификация – это процедура проверки подлинности входящего в систему объекта(пользователя), редьавившего

Аутентификация и идентификация являются взаимосвязанными процессами для определения и проверки подлинности пользователей системы. Именно от них зависит дальнейшее решение системы о том, какие действия следует предпринимать для предоставления ресурсов пользователю. Следует уточнить, что решение о предоставлении доступа зависит от используемой информационной системы.

Также стоит ввести понятие строгой аутентификации. Идея строгой аутентификации заключается в том, что проверяемая сторона доказывает свою подлинность проверяющей стороне на основе

какого-либо секрета, который предварительно был размещен на обеих сторонах. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.

Основополагающим является тот факт, что проверяемая сторона не передает свой секрет, аутентификация обеспечивается ответами доказывающей стороны на сгенерированные вопросы проверяющей стороны. В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов: – односторонняя аутентификация – двусторонняя аутентификация – трехсторонняя аутентификация. Односторонняя аутентификация предусматривает обмен информацией только в одном направлении. Двусторонняя аутентификация, по сравнению с односторонней, содержит дополнительный ответ проверяющей стороны. Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей.

Ещё до появления компьютеров использовались различные отличительные черты субъекта, его характеристики. Сейчас использование той или иной характеристики в системе зависит от требуемой надёжности, защищённости и стоимости внедрения. Выделяют три фактора аутентификации:

Фактор знания: что-то, что мы знаем — пароль. Это тайные сведения, которыми должен обладать только авторизованный субъект. Паролем может быть речевое слово, текстовое слово, комбинация для замка или личный идентификационный номер (PIN). Парольный механизм может быть довольно легко реализован и имеет низкую стоимость. Однако он имеет существенные недостатки: сохранить пароль в тайне зачастую бывает сложно, злоумышленники постоянно придумывают новые способы кражи, взлома и подбора пароля (см. бандитский криптоанализ, метод грубой силы). Это делает парольный механизм слабозащищённым. Многие секретные вопросы, такие как «Где вы родились?», элементарные примеры фактора знаний, потому что они могут быть известны широкой группой людей или быть исследованы. Из-за малой энтропии пользовательских паролей во всех системах регистрации и аутентификации пользователей применяется специальная политика безопасности. Типичные минимальные требования: Длина пароля от 8 символов. Использование разных регитров и небуквенных символов в паролях. Запрет паролей из словаря или часто используемых паролей. Ограниченное время действия пароля. Обязательная смена пароля по истечении срока действия. Блокирование возможности аутентификации после нескольких неудачных попыток.

Фактор владения: что-то, что мы имеем — устройство аутентификации. Здесь важно обстоятельство обладания субъектом каким-то неповторимым предметом. Это может быть личная печать, ключ от замка, для компьютера это файл данных, содержащих характеристику. Характеристика часто встраивается в особое устройство аутентификации, например пластиковую карту, смарт-карту. Для злоумышленника заполучить такое устройство более сложно, чем взломать пароль, а субъект может сразу же сообщить в случае кражи устройства. Это делает данный метод более защищённым, чем парольный механизм, однако стоимость такой системы более высокая.

Фактор свойства: что-то, что является частью нас — биометрия. Характеристикой является физическая особенность субъекта. Это может быть портрет, отпечаток пальца или ладони, голос или особенность глаза. С точки зрения субъекта, данный способ является наиболее простым: не надо ни запоминать пароль, ни переносить с собой устройство аутентификации. Однако биометрическая система должна обладать высокой чувствительностью, чтобы подтверждать авторизованного пользователя, но отвергать злоумышленника со схожими биометрическими параметрами. Также стоимость такой системы довольно велика. Но, несмотря на свои недостатки, биометрика остается довольно перспективным фактором.

Источник: <https://bit.ly/3doPVr4>

Источник: Криптографические методы защиты информации. Учебное пособие. Владимиров С. М., Габидулин Э. М., Колыбельников А. И., Кшевецкий А. С.

#### **4.2.2 Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС**

СУБД Oracle предоставляет следующие способы аутентификации пользователей:

1. Аутентификация средствами операционной системы. Некоторые ОС позволяют СУБД Oracle использовать информацию о пользователях, которыми управляет собственно ОС. В этом случае пользователь компьютера имеет доступ к ресурсам БД без дополнительного указания имени и пароля – используются его сетевые учетные данные. Данный вид аутентификации считается небезопасным и используется, в основном, для аутентификации администратора СУБД.
2. Аутентификация при помощи сетевых сервисов. Данный вид аутентификации обеспечивает опция сервера Oracle Advanced Security. Она предоставляет возможность SSL-аутентификации, а так же аутентификацию с помощью служб третьих сторон, в роли которых могут выступать Kerberos, PKI, RADIUS или служба LDAP-каталога.
3. Аутентификация в многоуровневых приложениях. Приведенные выше методы аутентификации также могут быть применены и в многоуровневых приложениях. Как правило, для доступа к приложениям из сети Интернет используется аутентификация по имени и паролю (в том числе с использованием протокола RADIUS), либо по протоколу SSL. Прочие методы используются для работы пользователей в локальной сети.

Источник : <http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/obespechenie-zaschity-personaln%h-dannyh-v-subd-oracle>

Аутентификация в Windows и хранение паролей:

ОС Windows, начиная с Vista, Server 2008, Windows 7, сохраняет пароли в виде NT-хэша, который вычисляется как 128-битовый хэш MD4 от пароля в Unicode кодировке. NT-хэш не использует «соль», поэтому применима словарная атака. На словарной атаке основаны программы поиска (взлома) паролей для Windows. Файл паролей называется SAM (англ. Security Account Manager) в случае локальной аутентификации. Если пароли хранятся на сетевом сервере, то они хранятся в специальном файле, доступ к которому ограничен. В последнем протоколе аутентификации NTLMv2 пользователь для входа в свой компьютер аутентифицируется либо локально на компьютере, либо удалённым сервером, если учётная запись пользователя хранится на сервере. Пользователь с именем user вводит пароль в программу-клиент, которая, взаимодействуя с программой-сервером (локальной или удалённой на сервере домена domain), аутентифицирует пользователя для входа в систему. Протокол аутентификации NTLMv2 обеспечивает одностороннюю аутентификацию пользователя серверу (или своему ПК). При удалённой аутентификации по сети последние версии Windows используют протокол Kerberos, который обеспечивает взаимную аутентификацию, и, только если аутентификация по Kerberos не поддерживается клиентом или сервером, она происходит по NTLMv2.

Источник: Криптографические методы защиты информации. Учебное пособие. Владимиров С. М., Габидулин Э. М., Колыбельников А. И., Кшевецкий А. С.

## 4.3 Средства управления доступом

### 4.3.1 Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления.

Сначала приведем формальные определения субъекта и объекта доступа:

Субъект доступа – активная сущность АС (автоматизированной системы), которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов.

Объект доступа – пассивная сущность АС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов. Теперь "по пацански чисто для понимания (хотя и неверно):

- Объект – ресурс АС к которой обращается субъект (информация)
- Субъект – пользователь

Группа - это именованная совокупность пользователей

Роль – набор прав (полномочий, привилегий) или ролей

Привилегии – права доступа, предоставляемые субъекту (тут нужно прям уточнить в лоб - привилегия дается СУБЪЕКТУ)

Представления - это специфический образ таблицы или набора таблиц, определенный оператором SELECT. В отличие от обычных таблиц реляционных баз данных, представление не является самостоятельной частью набора данных, хранящегося в базе. Содержимое представления динамически вычисляется на основании данных, находящихся в реальных таблицах. Изменение данных в реальной таблице базы данных немедленно отражается в содержимом всех представлений, построенных на основании этой таблицы. Некоторые СУБД имеют расширенные представления для данных, доступных только для чтения. Так, СУБД Oracle реализует концепцию «материализованных представлений» — представлений, содержащих предварительно выбранные неvirtуальные наборы данных, совместно используемых в распределённых БД. Эти данные извлекаются из различных удалённых источников (с разных серверов распределённой СУБД). Целостность данных в материализованных представлениях поддерживается за счёт периодических синхронизаций или с использованием триггеров. Аналогичный механизм предусмотрен в Microsoft SQL Server версии 2000.

По самой сути представления могут быть доступны только для чтения. Тем не менее, в некоторых СУБД (например, в Oracle) представления могут быть редактируемыми, как и обычные физические таблицы.

### 4.3.2 Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей.

Привилегии в СУБД можно подразделить на две категории: привилегии безопасности и привилегии доступа. Привилегии безопасности позволяют выполнять административные действия. Привилегии доступа, в соответствии с названием, определяют права доступа субъектов к определенным объектам.

Привилегии безопасности всегда выделяются конкретному пользователю (а не группе, роли или всем) во время его создания (оператором CREATE USER) или изменения характеристик (оператором ALTER USER). Примеры таких привилегий в СУБД INGRES:

- security - право управлять безопасностью СУБД и отслеживать действия пользователей. Пользователь с этой привилегией может подключаться к любой базе данных, создавать, удалять и изменять характеристики пользователей, групп и ролей, передавать права на доступ к базам данным другим пользователям, управлять записью регистрационной информации, отслеживать запросы других пользователей.
- createdb - право на создание и удаление баз данных. Этой привилегией, помимо администратора сервера, должны обладать пользователи, которым отводится роль администраторов отдельных баз данных.
- operator - право на выполнение действий, которые традиционно относят к компетенции оператора. Имеются в виду запуск и остановка сервера, сохранение и восстановление информации. Помимо администраторов сервера и баз данных этой привилегией целесообразно наделить также администратора операционной системы.
- maintain\_locations - право на управление расположением баз администратора сервера баз данных и операционной системы.

Привилегии доступа выделяются пользователям, группам, ролям или всем посредством оператора GRANT и изымаются с помощью оператора REVOKE. Эти привилегии, как правило, присваивает владелец соответствующих объектов (он же - администратор базы данных) или обладатель привилегии security (обычно администратор сервера баз данных).

Прежде чем присваивать привилегии группам и ролям, их (группы и роли) необходимо создать с помощью операторов CREATE GROUP и CREATE ROLE.

Для изменения состава группы служит оператор ALTER GROUP. Оператор DROP GROUP позволяет удалять группы, правда, только после того, как опустошен список членов группы. Оператор ALTER ROLE служит для изменения паролей ролей, а DROP ROLE - для удаления ролей.

Создавать и удалять именованные носители привилегий, а также изменять их характеристики может лишь пользователь с привилегией security. При совершении подобных действий необходимо иметь подключение к базе данных, в которой хранятся сведения о субъектах и их привилегиях.

#### 4.3.3 Соотношение прав доступа СУБД и операционной системы

Данные, хранящиеся средствами СУБД, располагаются в файлах и/или логических томах операционной системы. Соответственно, и доступ к этим данным возможен как с помощью СУБД, так и посредством утилит ОС. Так называемая естественная защита баз данных, являющаяся следствием относительно сложного формата их хранения, едва ли способна остановить злоумышленника.

Чтобы средствами ОС нельзя было скомпрометировать базу данных и сопутствующую информацию, например журналы транзакций, необходимо установить максимально жесткий режим доступа к соответствующим файлам и томам. Для UNIX-систем целесообразно предоставить право непосредственного доступа только пользователям root, ingres и, быть может, администраторам баз данных. Все прочие субъекты должны осуществлять доступ к базам с помощью программ со взведенным битом переустановки действующего идентификатора пользователя. Данные из базы могут

экспортироваться в файлы операционной системы или другие хранилища. Возможен и обратный процесс импорта данных. Необходимо следить за тем, чтобы подобные операции не понижали уровня защищенности информации. Сделать это, вообще говоря, непросто. Во-первых, операционная система (например, персонального компьютера) может не обеспечивать должной защиты. Во-вторых, даже для развитых ОС необходимо установить и поддерживать соответствие между механизмами защиты СУБД и операционных систем. При большом числе пользователей (порядка нескольких сотен) данная задача становится очень сложной. Видимо, наиболее практичное решение сводится к административному контролю за экспортом/импортом информации. Можно предположить, что исходные тексты сколько-нибудь сложных процедур баз данных будут храниться в файлах операционной системы, формально не имеющих отношения к СУБД. Потенциально возможно нелегальное изменение исходного текста, которое, как было показано ранее, способно привести к серьезным нарушениям информационной безопасности. Вероятно, и здесь лучшим средством является административный контроль за размещением процедур в базах данных и за передачей прав на их выполнение. СУБД и ОС предлагают во многом сходные средства защиты данных. Более того, многие СУБД просто полагаются на операционную систему в плане идентификации и проверки подлинности пользователей. Тем не менее даже для таких "дружественных" сервисов проведение в жизнь согласованной политики безопасности является очень сложным делом. На практике приходится всячески ограничивать информационный обмен между СУБД и ОС.

#### **4.3.4 Метки безопасности.**

В "Критериях оценки надежных компьютерных систем" применительно к системам уровня безопасности описан механизм меток безопасности, реализованный в версии INGRES/ Enhanced Security (INGRES с повышенной безопасностью). Применять эту версию на практике имеет смысл только в сочетании с операционной системой и другими программными компонентами того же уровня безопасности. Тем не менее рассмотрение реализации меточной безопасности в СУБД INGRES интересно с познавательной точки зрения, а сам подход, основанный на разделении данных по уровням секретности и категориям доступа, может оказаться полезным при проектировании системы привилегий многочисленных пользователей по отношению к большим массивам данных.

В СУБД INGRES/Enhanced Security к каждой реляционной таблице неявно добавляется столбец, содержащий метки безопасности строк таблицы. Метка безопасности состоит из трех компонентов:

- уровень секретности. Смысл этого компонента зависит от приложения. В частности, возможен традиционный спектр уровней от "совершенно секретно" до "несекретно";
- категории. Понятие категории позволяет разделить данные на "отсеки" и тем самым повысить надежность системы безопасности. В коммерческих приложениях категориями могут служить "финансы" "кадры" "материальные ценности" и т.п. Ниже назначение категорий разъясняется более подробно;
- области. Является дополнительным средством деления информации на отсеки. На практике компонент "область" может действительно иметь географический смысл, обозначая, например, страну, к которой относятся данные. Каждый пользователь СУБД INGRES/ Enhanced Security характеризуется степенью благонадежности, которая также определяется меткой безопасности, присвоенной данному пользователю. Пользователь может получить доступ к данным, если степень его благонадежности удовлетворяет требованиям соответствующей метки безопасности. Более точно:
- уровень секретности пользователя должен быть не ниже уровня секретности данных;
- набор категорий, заданных в метке безопасности данных, должен целиком содержаться в метке безопасности пользователя;
-



набор областей, заданных в метке безопасности пользователя, должен целиком содержаться в метке безопасности данных.

Рассмотрим ГИПОТЕТИЧЕСКИЙ пример И НИКОГО НЕ ИМЕЕМ ВВИДУ, ВСЕ ПЕРСОНАЖИ И СОБЫТИЯ ЯВЛЯЮТСЯ ФАНТАЗИЕЙ БОЛЬНОЙ ГОЛОВЫ АВТОРА. Пусть данные о том, ехал человек в поезде или нет имеют уровень секретности "для служебного пользования" принадлежат категории "поезда" и "пассажиры" и относятся к областям "Москва" и "Татарстан". Далее, пусть степень благонадежности пользователя характеризуется меткой безопасности с уровнем секретности "для служебного пользования" категориями "поезда" и "самолеты" а также областью "Москва" и "Татарстан". Такой пользователь не получит доступ к данным, в метке пользователя была указана только категория "поезда" (без категории "пассажиры"), в доступе к данным ему было бы отказано.

Когда пользователь производит выборку данных из таблицы, он получает только те строки, меткам безопасности которых удовлетворяет степень его благонадежности. Для совместимости с обычными версиями СУБД, столбец с метками безопасности не включается в результирующую информацию.

Отметим, что механизм меток безопасности не отменяет, а дополняет произвольное управление доступом. Пользователи по-прежнему могут оперировать таблицами только в рамках своих привилегий, но даже при наличии привилегии SELECT им доступна, вообще говоря, только часть данных.

При добавлении или изменении строк они, как правило, наследуют метки безопасности пользователя, инициировавшего операцию. Таким образом, даже если авторизованный пользователь переписшет секретную информацию в общедоступную таблицу, менее благонадежные пользователи не смогут ее прочитать.

Специальная привилегия, DOWNGRADE, позволяет изменять метки безопасности, ассоциированные с данными. Подобная возможность необходима, например, для коррекции меток, по тем или иным причинам оказавшихся неправильными.

Представляется естественным, что СУБД INGRES/Enhanced Security допускает не только скрытое, но и явное включение меток безопасности в реляционные таблицы. Появился новый тип данных, security label, поддерживающий соответствующие операции сравнения.

#### **4.3.5 Использование представлений для обеспечения конфиденциальности информации в СУБД.**

СУБД предоставляют специфическое средство управления доступом - представления. Представления позволяют сделать видимыми для субъектов определенные столбцы базовых таблиц (реализовать проекцию) или отобрать определенные строки (реализовать селекцию). Не предоставляя субъектам прав доступа к базовым таблицам и сконструировав подходящие представления, администратор базы данных защитит таблицы от несанкционированного доступа и снабдит каждого пользователя своим видением базы данных, когда недоступные объекты как бы не существуют.

Приведем пример создания представления, содержащего два столбца исходной таблицы и включающего в себя только строки с определенным значением одного из столбцов:

```
CREATE VIEW empview AS  
SELECT name, dept
```

```
FROM employee
WHERE dept = "shoe";
```

Предоставим всем право на выборку из этого представления:

```
GRANT SELECT
ON empview
TO PUBLIC;
```

Субъекты, осуществляющие доступ к представлению empview, могут пытаться запросить сведения об отделах, отличных от shoe, например:

```
SELECT *
FROM empview
WHERE dept = "toy";
```

но в ответ просто получают результат из нуля строк, а не код ответа, свидетельствующий о нарушении прав доступа. Это принципиально важно, так как лишает злоумышленника возможности получить список отделов косвенным образом, анализируя коды ответов, возвращаемые после обработки SQL-запросов.

#### 4.4 Обеспечение конфиденциальности путем тиражирования БД

Тиражирование (репликация) – технология, предусматривающая поддержку копий всей БД или ее фрагментов в нескольких узлах сети. Копия БД называется репликой. Копии БД обычно приближены к местам использования информации. В контексте информационной безопасности тиражирование можно рассматривать как средство повышения доступности данных. Стала легендой история про бакалейщика из Сан-Франциско, который после разрушительного землетрясения восстановил свою базу данных за 16 минут, перекачав из другого города предварительно протиражированную информацию.

Развитые возможности тиражирования предоставляет СУБД INGRES. Им посвящена статья [2]. Здесь мы рассмотрим возможности другого популярного сервера СУБД - Informix OnLine Dynamic Server (OnLine-DS) 7.1. В отличие от предыдущего раздела, речь пойдет об обычных (а не кластерных) конфигурациях. В Informix OnLine-DS 7.1 поддерживается модель тиражирования, состоящая в полном отображении данных с основного сервера на вторичные.

В конфигурации серверов Informix OnLine-DS с тиражированием выделяется один основной и ряд вторичных серверов. На основном сервере выполняется и чтение, и обновление данных, а все изменения передаются на вторичные серверы, доступные только на чтение. В случае отказа основного сервера вторичный автоматически или вручную переводится в режим доступа на чтение и запись. Прозрачное перенаправление клиентов при отказе основного сервера не поддерживается, но оно может быть реализовано в рамках приложений.

После восстановления основного сервера возможен сценарий, при котором этот сервер становится вторичным, а бывшему вторичному, который уже функционирует в режиме чтения-записи, придается статус основного; клиенты, которые подключены к нему, продолжают работу. Таким образом, обеспечивается непрерывная доступность данных. Тиражирование осуществляется путем передачи информации из журнала транзакций (логического журнала) в буфер тиражирования основного сервера, откуда она пересылается в буфер тиражирования вторичного сервера. Такая

пересылка может происходить либо в синхронном, либо в асинхронном режиме. Синхронный режим гарантирует полную согласованность баз данных - ни одна транзакция, зафиксированная на основном сервере, не останется незафиксированной на вторичном, даже в случае сбоя основного сервера. Асинхронный режим не обеспечивает абсолютной согласованности, но улучшает рабочие характеристики системы.

Побочный положительный эффект тиражирования - возможность вынести преимущественно на вторичный сервер ресурсоемкие приложения поддержки принятия решений. В этом случае они могут выполняться с максимальным использованием средств параллельной обработки, не подавляя приложений оперативной обработки транзакций, сосредоточенных на основном сервере. Это также можно рассматривать как фактор повышения доступности данных.

Формальная модель для обеспечения конфиденциальности БД с помощью тиражирования. Вот не нашел источников под это. Архитектура и политика безопасности в модели SINTRA.

<https://bit.ly/2U0iaoi>

глава 4 на англуйцком было слажна и предлагается читателю перевести это самому

## 4.5 Аудит и подотчетность

Регистрация действий пользователей, так или иначе влияющих на информационную безопасность, является фактором, сдерживающим потенциальных злоумышленников и позволяющим расследовать уже случившиеся нарушения.

Более точно, журнал регистрационной информации может использоваться для следующих целей:

- обнаружение необычных или подозрительных действий пользователей и идентификации лиц, совершающих эти действия;
- обнаружение попыток несанкционированного доступа
- оценка возможных последствий состоявшегося нарушения информационной безопасности
- оказание помощи в расследовании случаев нарушения безопасности
- организация пассивной защиты от нелегальных действий. Пользователи, зная, что их действия фиксируются, могут не решиться на незаконные операции. Чтобы данная цель достигалась, необходимо довести до сведения каждого пользователя, что каждое его действие регистрируется и что за незаконные операции он может понести наказание.

### 4.5.1 Подотчетность действий пользователя и аудит связанных с безопасностью событий.

Протоколирование, или регистрация, представляет собой механизм подотчётности системы обеспечения информационной безопасности, фиксирующий все события, относящиеся к вопросам безопасности. В свою очередь, аудит – это анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности.

Не менее важен вопрос о порядке хранения системных журналов. Поскольку файлы журналов хранятся на том или ином носителе, неизбежно возникает проблема переполнения максимально

допустимого объёма системного журнала. При этом реакция системы может быть различной, например:

- система может быть заблокирована вплоть до решения проблемы с доступным дисковым пространством
- могут быть автоматически удалены самые старые записи системных журналов
- система может продолжить функционирование, временно приостановив протоколирование информации

Безусловно, последний вариант в большинстве случаев является неприемлемым, и порядок хранения системных журналов должен быть чётко регламентирован в политике безопасности организации.

В терминологии регистрационной службы любое действие, способное изменить состояние базы данных, называется событием и может регистрироваться. В СУБД Informix события обозначаются четырёхбуквенными мнемониками. Приведем несколько событий безопасности:

- ACTB - доступ к таблице
- CLDB - закрытие таблицы
- DRTB - удаление таблицы

#### **4.5.2 Регистрация действий пользователя**

Регистрация всех событий для всех пользователей существенно снизит эффективность работы СУБД. Администратор СУБД (или лицо, отвечающее за информационную безопасность) должен выбрать приемлемый баланс между безопасностью и эффективностью. Рекомендуется регистрировать по крайней мере следующие события:

- передача привилегий доступа к базе данных (GRDB)
- лишение привилегий доступа к базе данных (RVDB)
- передача привилегий доступа к таблице (GRTB)
- лишение привилегий доступа к таблице (RVTB)
- открытие базы данных (OPDB)

Перечисленные события происходят нечасто, однако их фиксация позволяет составить представление о том, чем интересуется каждый из пользователей. Если какой-либо пользователь замечен в подозрительных действиях, для него можно включить режим регистрации всех событий. Для администратора СУБД и лица, отвечающего за безопасность, подобный режим должен быть включен постоянно. Отметим, что у пользователя нет возможности узнать, какие из его действий регистрируются. Целесообразно поддерживать в нем уверенность, что регистрируется все или почти все.

### 4.5.3 Управление набором регистрируемых событий

Для управления набором регистрируемых событий в СУБД Informix используются маски событий. Три стандартные маски с именами `_default`, `_require` и `_exclude` формируют стандартное регистрационное окружение. Кроме того, для отдельных пользователей могут быть заданы персональные маски с именами, совпадающими с входными именами этих пользователей.

Результирующее регистрационное окружение пользователя формируется следующим образом: Берется маска `_default` или маска пользователя, если таковая имеется.

В число регистрируемых дополнительно включаются события, заданные маской `_require`. Из числа регистрируемых исключаются события, заданные маской `_exclude`, при условии, что они не были упомянуты в маске `_require`.

Таким образом, в СУБД Informix выполнено одно из требований к системам класса безопасности C2, предписывающее возможность задания своего перечня регистрируемых событий для каждого пользователя.

Маски можно формировать с помощью утилиты `onaudit`. Приведем пример командной строки, позволяющей добавить к маске `_default` регистрацию событий, вызываемых операциями со строками таблиц: `onaudit -m -u _default -e +DLRW,INRW,RDRW,UPRW`

С помощью утилиты `onaudit` можно выдать состояние той или иной маски, создать, модифицировать или удалить ее. Та же утилита (и это важно отметить) позволяет включать и выключать регистрацию событий сервером СУБД Informix.

### 4.5.4 Анализ регистрационной информации

- ONLN - фиксированное поле, обозначающее события, фиксируемые сервером Informix-OnLine
- дата и время события
- имя клиентского компьютера, инициировавшего событие
- идентификатор клиентского процесса, инициировавшего событие
- имя серверного компьютера
- имя пользователя
- код завершения действия, вызвавшего событие
- мнемоника события
- дополнительные поля, идентифицирующие базы данных, таблицы и другие объекты, вовлеченные в событие

С помощью утилиты `onshowaudit` можно отобразить часть регистрационной информации и организовать ее просмотр или, воспользовавшись утилитой `dbload`, загрузить ее в базу данных и анализировать затем SQL-средствами. Регистрационная служба СУБД Informix является субъектно-ориентированной в том смысле, что можно задать свой набор отслеживаемых событий для каждого пользователя (субъекта), однако нет возможности указать имена объектов (таблиц, процедур и т.п.), операции с которыми отслеживались бы особым образом. Вместо этого предлагается полагаться на

средства анализа регистрационной информации. Очевидно, после загрузки регистрационного журнала в базу данных можно отобрать сведения по сколь угодно сложному критерию и сгенерировать отчет, по существу, произвольного вида.

Регистрационные файлы и результат их загрузки в базу данных нуждаются в защите. В частности, для файлов рекомендуется установить в качестве владельца пользователя root, владеющей группой сделать informix, а режим доступа положить равным 0660 (доступ на чтение и запись только для владельца и группы).

Регистрационная информация нуждается в ежедневном анализе. В противном случае реакция на подозрительные действия или нарушения окажется запоздалой. В первом приближении подозрительными можно считать действия, завершившиеся ненормальным образом, то есть с ненулевым кодом. Более сложные эвристики могут опираться на статистический анализ спектра пользовательских действий. Как уже указывалось, после обнаружения подозрительной активности целесообразно включить режим регистрации всех действий пользователя и/или принять административные меры.

Источник на котором основана большая часть данной главы:

<https://www.osp.ru/news/articles/1996/0131/13031467>

## 5 Механизмы, поддерживающие высокую готовность

Определение: Высокая готовность (High Availability, HA) - это характеристика технической системы, разработанная для избежания невыполненного обслуживания путём уменьшения или управления сбоями и минимизации времени плановых простоев.

Высокая готовность для каждой конкретной системы зависит от цели, для которой предназначена эта система. Для некоторых компаний высокая готовность значит максимальное downtime за год в несколько минут. Для других HA может значит downtime несколько часов в месяц. Доступность(готовность) часто измеряется в «Nines»

Availability %	Downtime per year <sup>[note 1]</sup>	Downtime per month	Downtime per week	Downtime per day
<b>90% ("one nine")</b>	<b>36.53 days</b>	<b>73.05 hours</b>	<b>16.80 hours</b>	<b>2.40 hours</b>
95% ("one and a half nines")	18.26 days	36.53 hours	8.40 hours	1.20 hours
97%	10.96 days	21.92 hours	5.04 hours	43.20 minutes
98%	7.31 days	14.61 hours	3.36 hours	28.80 minutes
<b>99% ("two nines")</b>	<b>3.65 days</b>	<b>7.31 hours</b>	<b>1.68 hours</b>	<b>14.40 minutes</b>
99.5% ("two and a half nines")	1.83 days	3.65 hours	50.40 minutes	7.20 minutes

Рис. 2: Пример Nines. Взято из википедии

HA включает в себя несколько важных аспектов:

1. Доступность данных
2. Защита данных
3. Производительность
4. Цена поддержки

## 5.1 Средства, поддерживающие высокую готовность

**Аппаратная и программная поддержки** Существует несколько возможных уровней обеспечения высокой готовности системы: аппаратный и программный уровни.

Аппаратный уровень включает в себя:

1. Репликация БД Репликация позволяет скопировать данные с одного сервера бд на другой. Существуют два подхода репликации баз данных, рассмотрим каждый из них:

- Репликация Master-Slave

В этом подходе выделяется один основной сервер базы данных, который называется Мастером. На нем происходят все изменения в данных (любые запросы INSERT/UPDATE/DELETE). Слейв сервер постоянно копирует все изменения с Мастера. С приложения на Слейв сервер могут отправляться запросы на чтение данных (запросы SELECT). Таким образом Мастер сервер может отвечать за изменения данных, а Слейв за чтение. Также Мастер сервер может отвечать за все операции с данными, а Слейв являться бэкапом. При выходе из строя Слейва, достаточно просто переключить все приложение на работу с Мастером. После этого восстановить репликацию на Слейве и снова его запустить. Если выходит из строя Мастер, нужно переключить все операции (и чтения и записи) на Слейв. Таким образом он станет новым Мастером. После восстановления старого Мастера, настроить на нем реплику, и он станет новым Слейвом. Рассмотрена асинхронная репликация. При синхронной репликации результат сразу же записывается и в Мастер и в Слейв. Возвращение управления клиенту происходит только после записи в обе базы.

- Репликация Master-Master

В этой схеме, любой из серверов может использоваться как для чтения так и для записи. При использовании такого типа репликации достаточно выбирать случайное соединение из доступных Мастеров. Вероятные поломки делают Master-Master репликацию непривлекательной. Выход из строя одного из серверов практически всегда приводит к потере каких-то данных. Последующее восстановление также сильно затрудняется необходимостью ручного анализа данных, которые успели либо не успели скопироваться.

Как уже говорилось ранее, репликацию данных можно разделить на синхронную и асинхронную. При асинхронной репликации изменения в slave или 2 master могут появляться с задержкой. При синхронной репликации может существовать только одна версия данных, что накладывает ограничения на работу с данными в процессе репликации.

Существует логическая репликация. Логическая репликация — это метод репликации объектов данных и изменений в них, использующий репликационные идентификаторы (обычно это первичный ключ). Мы называем такую репликацию «логической», в отличие от физической, которая построена на точных адресах блоков и побайтовом копировании. PostgreSQL поддерживает оба механизма одновременно; Логическая репликация позволяет более детально управлять репликацией данных и аспектами безопасности.

В логической репликации используется модель публикаций/подписок с одним или несколькими подписчиками, которые подписываются на одну или несколько публикаций на публикующем узле. Подписчики получают данные из публикаций, на которые они подписаны, и могут

затем повторно опубликовать данные для организации каскадной репликации или более сложных конфигураций.

Логическая репликация таблицы обычно начинается с создания снимка данных в публикуемой базе данных и копирования её подписчику. После этого изменения на стороне публикации передаются подписчику в реальном времени, когда они происходят. Подписчик применяет изменения в том же порядке, что и узел публикации, так что для публикаций в рамках одной подписки гарантируется транзакционная целостность. Этот метод репликации данных иногда называется транзакционной репликацией.

2. RAID - технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и производительности. Рассмотрим базовые уровни рейд массивов:

2.1 RAID 0 (striping — «чередование») — дисковый массив из двух или более жёстких дисков без резервирования.

2.2 RAID 1 (mirroring — «зеркалирование») — массив из двух (или более) дисков, являющихся полными копиями друг друга. Не следует путать с массивами RAID 1+0 (RAID 10), RAID 0+1 (RAID 01), в которых используются более сложные механизмы зеркалирования.

2.3 RAID 2. Массивы такого типа основаны на использовании кода Хэмминга. Диски делятся на две группы: для данных и для кодов коррекции ошибок, причём если данные хранятся на  $2^n - n - 1$  дисках, то для хранения кодов коррекции необходимо  $n$  дисков. Суммарное количество дисков при этом будет равняться  $2^n - 1$ . Данные распределяются по дискам, предназначенным для хранения информации, так же, как и в RAID 0, то есть они разбиваются на небольшие блоки по числу дисков.

2.4 В массиве RAID 3 из  $n$  дисков данные разбиваются на куски размером меньше сектора (разбиваются на байты или блоки) и распределяются по  $n - 1$  дискам. Ещё один диск используется для хранения блоков чётности. В RAID 2 для этой цели применялся  $n - 1$  диск, но большая часть информации на контрольных дисках использовалась для коррекции ошибок «на лету», в то же время большинство пользователей устраивает простое восстановление информации в случае её повреждения, для чего хватает данных, уместяющихся на одном выделенном жёстком диске.

Отличия RAID 3 от RAID 2: невозможность коррекции ошибок на лету.

2.5 RAID 4 похож на RAID 3, но отличается от него тем, что данные разбиваются на блоки, а не на байты. Таким образом, удалось отчасти «победить» проблему низкой скорости передачи данных небольшого объёма. Запись же производится медленно из-за того, что чётность для блока генерируется при записи и записывается на единственный диск.

2.6 RAID 5. Основным недостатком уровней RAID от 2-го до 4-го является невозможность производить параллельные операции записи, так как для хранения информации о чётности используется отдельный контрольный диск. RAID 5 не имеет этого недостатка. Блоки данных и контрольные суммы циклически записываются на все диски массива, нет асимметричности конфигурации дисков. Под контрольными суммами подразумевается результат операции XOR (исключающее или). Хог обладает особенностью, которая



даёт возможность заменить любой операнд результатом, и, применив алгоритм хог, получить в результате недостающий операнд.

2.7 RAID 6 — похож на RAID 5, но имеет более высокую степень надёжности — два (или более) диска данных и два диска контроля чётности. Основан на кодах Рида — Соломона и обеспечивает работоспособность после одновременного выхода из строя любых двух дисков. Обычно использование RAID 6 вызывает примерно 10-15 % падение производительности дисковой группы, относительно RAID 5, что вызвано большим объёмом работы для контроллера (более сложный алгоритм расчёта контрольных сумм), а также необходимостью читать и перезаписывать больше дисковых блоков при записи каждого блока.

Также существуют различные комбинации данных подходов.

#### Программные подходы:

1. Автоматический перезапуск экземпляров БД, сетевых демонов и других ресурсов
2. Защита от повреждения данных(Data corruption protection)
  - Использование контрольных чек-сумм
  - Автоматическое восстановление из резервной копии или повторная передача
3. PITR (Point In Time Recovery) Данный механизм позволяет восстановить базу данных в том виде, в котором она была в каком-то моменте в прошлом.
4. Application continuity (Oracle) Маскирует от приложения и конечных пользователей падение базы данных и позволяет восстановить сеансы базы данных во время работы.
5. WAL Данный подход будет описан ниже.

#### **Кластерная организация серверов баз данных**

Кластеризация базы данных - это процесс объединения нескольких серверов или инстансов, соединяющих одну базу данных. Иногда одного сервера может быть недостаточно для управления объемом данных или количеством запросов, тогда возникает необходимость в кластере.

К общим требованиям, предъявляемым к кластерным системам, относятся:

1. Высокая готовность
2. Высокое быстродействие
3. Масштабирование
4. Удобство обслуживания

Кластеры баз данных являются распространенной технологией. Рассмотрим три типа архитектуры кластерных вычислений. Отказоустойчивые кластеры, высокопроизводительные кластеры и кластеры балансировки нагрузки.

1. Отказоустойчивые / высокодоступные кластеры. Кластер обеспечивает доступность сервиса путем репликации серверов и избыточной реконфигурации программного и аппаратного обеспечения. Таким образом, каждая система контролирует другую и работает на запросы, если какой-либо один из узлов выходит из строя.
2. Высокопроизводительные кластеры. Целью разработки высокопроизводительных кластеров баз данных является создание высокопроизводительных компьютерных систем. Основная цель - разумное распределение рабочей нагрузки.
3. Кластеры балансировки нагрузки. Эти кластеры базы данных служат для распределения нагрузки между различными серверами. Они стремятся обеспечить увеличенную пропускную способность сети, в конечном итоге увеличивая производительность. Системы в этой сети объединяют свои узлы, с помощью которых пользовательские запросы равномерно распределяются между участвующими узлами.

Несмотря на всю распределенную систему на заднем плане, пользователю это кажется единой системой. Использование кластеров варьируется от предприятия к предприятию, в зависимости от вида процессов и требуемого уровня производительности.

### **Параметры настройки СУБД**

Непонятно о чем это, настройки чего

### **Сохранение и восстановление БД**

Основным свойством транзакций СУБД является durability. Идея механизма обеспечения этого свойства является одинаковой для всех СУБД. СУБД использует специальный лог (Write-Ahead Lock - WAL), в который записываются все транзакции, результат которых не попал на физический диск. WAL — это журнал опережающей записи, технология, которую часто используют для улучшения надежности базы данных. Когда вы заносите информацию в базу данных, база выполняет несколько операций, манипулируя блоками. Следовательно, с точки зрения файловой системы INSERT и UPDATE не являются атомарными операциями: если кто-то внезапно выключит ваш сервер, данные окажутся испорчены. Если возникает сбой, база данных использует этот файл для того, чтобы восстановить данные на момент падения. WAL – это бинарный лог, так что для его чтения нужна специальная утилита. Например в PostgreSQL данный файл называется WAL и лежит по пути `$PGDATA/pg_xlog`. PostgreSQL позволяет отключать WAL для отдельных таблиц, помечая их как UNLOGGED.

## **5.2 Оперативное администрирование**

**Задачи, средства и режимы администрирования** Задачи администратора баз данных могут незначительно отличаться в зависимости от вида применяемой СУБД, но в основные задачи входит:

- Проектирование базы данных.
- Оптимизация производительности базы данных.
- Резервирование и восстановление базы данных.

- Обеспечение целостности баз данных.
- Обеспечение перехода на новую версию СУБД.

Существуют различные программы и способы администрирования БД, которые напрямую зависят от БД. Основным инструментом работы с базой данных является DSL и программы, например для Oracle можно использовать SQL Developer. Существуют программы, поддерживающие работу с любой БД, например продукты JetBrains. Также отдельно существуют средства мониторинга серверов.

**Мониторинг серверов СУБД** Мониторинг СУБД можно условно разделить на два типа:

1. Мониторинг средствами СУБД
2. Мониторинг хостов, на которых запущена БД.

#### Мониторинг средствами СУБД

Средства мониторинга, предоставляемые СУБД зависят в первую очередь от конкретной реализации этой системы, однако можно выделить метрики, которые в большинстве случаев собираются встроенным мониторингом. В первую очередь это объем операций ввода/вывода, необходимых для исполнения транзакции, утилизация процессоров и временем отклика системы. Наиболее распространенной метрикой оценки производительности системы является ее время отклика, которое представляет собой интервал времени, в течении которого сервер возвращает первую строку результата исполнения запроса, т.е. пользователь получает визуальное подтверждение того, что его запрос исполняется. Пропускная способность обслуживаемых сервером процессов и пользователей определяет сколько запросов возможно исполнить в фиксированный интервал времени, и сколько строк и какого размера возвращается клиенту. При увеличении числа активных процессов и/или пользователей, возрастает и их конкуренция за системные ресурсы. Результатом такой чрезмерной нагрузки может стать увеличение времени отклика и снижение общей пропускной способности. Большое влияние на производительности базы данных оказывает также физическая и логическая целостность данных.

#### Мониторинг хостов, на которых запущена БД.

Многофункциональным средством является Zabbix —свободная система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Он поддерживает несколько видов мониторинга. Simple checks —может проверять доступность и реакцию стандартных сервисов, таких как SMTP или HTTP без установки какого-либо программного обеспечения на наблюдаемом хосте. Zabbix agent — может быть установлен на UNIX-подобных или Windows хостах для получения данных о нагрузке процессора, использования сети, дисковом пространстве и так далее. External check — выполнение внешних программ. Zabbix также поддерживает мониторинг через SNMP. Благодаря расширяемости данная система мониторинга позволяет контролировать любые метрики системы. К недостаткам можно отнести некоторую трудоемкость при необходимости слежения за нестандартными параметрами системы. Для мониторинга систем чаще всего используется протокол SNMP, и можно сказать, что он являлся долгое время стандартом де факто. Протокол SNMP работает на базе протокола UDP и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию,

изменять, посылать «trap» на сервер мониторинга. Протокол определяет формат данных, их обработка и интерпретация остаются на усмотрение системного администратора и системы мониторинга. SNMP-сообщения не имеют фиксированного формата и фиксированных полей. Как следствие протокол SNMP универсален, но его главным недостатком является дополнительный трафик и необходимость загружать резидентные продукты (агенты) на управляемых объектах.

### 5.3 Функциональная насыщенность СУБД

**Формы избыточности** Системы, обеспечивающие непрерывный доступ к данным (fault tolerant) или почти непрерывный (high availability) обычно опираются на различные формы избыточности. Как правило, это системы дублирования аппаратного обеспечения и контролируемой избыточности данных.

**Аппаратная избыточность** Аппаратная избыточность может включать платформы с полным резервированием, поддерживающие (standby) процессоры, диски с двойным интерфейсом (dual-port), дисковые массивы и пр. Один из вариантов - зеркалирование дисков, когда один диск используется в качестве копии другого и может быть использован при сбое вместо него. Хотя аппаратная избыточность и важна для повышения общей надежности системы, ее реализация, как правило, не ориентирована на обработку транзакций СУБД и на связанные с этим специфические ограничения, например, обеспечение атомарности транзакции. В результате СУБД не может воспользоваться преимуществами чисто аппаратных решений резервирования системы для повышения своей производительности.

**Избыточность данных** Нормальная форма — свойство отношения в реляционной модели данных, характеризующее его с точки зрения избыточности, потенциально приводящей к логически ошибочным результатам выборки или изменения данных. Нормальная форма определяется как совокупность требований, которым должно удовлетворять отношение.

Процесс преобразования отношений базы данных к виду, отвечающему нормальным формам, называется нормализацией. Нормализация предназначена для приведения структуры БД к виду, обеспечивающему минимальную логическую избыточность, и не имеет целью уменьшение или увеличение производительности работы или же уменьшение или увеличение физического объема базы данных. Конечной целью нормализации является уменьшение потенциальной противоречивости хранимой в базе данных информации. Как отмечает К. Дейт, общее назначение процесса нормализации заключается в следующем:

- исключение некоторых типов избыточности;
- устранение некоторых аномалий обновления;
- разработка проекта базы данных, который является достаточно «качественным» представлением реального мира, интуитивно понятен и может служить хорошей основой для последующего расширения;
- упрощение процедуры применения необходимых ограничений целостности.

Устранение избыточности производится, как правило, за счёт декомпозиции отношений таким образом, чтобы в каждом отношении хранились только первичные факты (то есть факты, не выводимые из других хранимых фактов).  
Существуют 6 нормальных форм.

**Программное зеркалирование** Программное зеркалирование дисков, называемое также дуплексированием (duplexing) или мультиплексированием (multiplexing), может не только защитить от аппаратных сбоев, но и улучшить производительность. Поскольку зеркалирование базы данных (или ее частей - таблиц(ы), индексов, их фрагментов и пр.) производится на другом физическом устройстве, то операции чтения данных можно распределить между двумя устройствами и производить параллельно (рис. 2). Конечно, зеркалирование бесполезно с любой точки зрения, если оно организовано на одном диске. В случае повреждения зеркалируемого диска все операции автоматически переносятся на исправный диск, сбойный диск выводится в отключенное состояние, причем приложения не замечают каких-либо изменений в конфигурации системы. После замены неисправного диска параллельно с работой пользователей запускается процесс оперативной синхронизации зеркальных дисков (on-line remirroring), на физическом уровне копирующий рабочий диск.

**Тиражирование данных** Тиражирование в системах, требующих в первую очередь повышенной надежности, в целом подобно зеркалированию, но здесь копия данных может поддерживаться удаленно. Если происходит копирование всей базы данных, то обычно это делается с целью обеспечить горячий резерв (warm standby). Однако в некоторых реализациях есть возможность использовать копию для просмотра (без модификации) данных. Это способно обеспечить значительные преимущества для систем со смешанной загрузкой, поскольку приложения для принятия решений, генерации отчетов и т.п. могут обращаться к копии базы данных, в то время как приложения оперативной обработки транзакций используют первичную базу данных.

## 5.4 Системы, обладающие свойством высокой готовности

### Описание, назначение, примеры

Cassandra - распределённая система управления базами данных, относящаяся к классу NoSQL-систем и рассчитанная на создание высокомасштабируемых и надёжных хранилищ огромных массивов данных, представленных в виде хэша.

Хранилище само позаботится о проблемах наличия единой точки отказа (single point of failure), отказа серверов и о распределении данных между узлами кластера (cluster node). При чем, как в случае размещения серверов в одном центре обработки данных (data center), так и в конфигурации со многими центрами обработки данных, разделенных расстояниями и, соответственно, сетевыми задержками. Под надёжностью понимается итоговая согласованность (eventual consistency) данных с возможностью установки уровня согласования данных (tune consistency) каждого запроса.

Узлы кластера кассандры равноценны, и клиенты могут соединиться с любым из них, как для записи, так и для чтения. Запросы проходят стадию координации, во время которой, выяснив при помощи ключа и разметчика на каких узлах должны располагаться данные, сервер посылает запросы к этим узлам. Будем называть узел, который выполняет координацию — координатором

(coordinator), а узлы, которые выбраны для сохранения записи с данным ключом — узлами-реплик (replica nodes). Физически координатором может быть один из узлов-реплик — это зависит только от ключа, разметчика и меток. Для каждого запроса, как на чтение, так и на запись, есть возможность задать уровень согласованности данных.

Когда данные приходят после координации на узел непосредственно для записи, то они попадают в две структуры данных: в таблицу в памяти (memtable) и в журнал закрепления (commit log). Таблица в памяти существует для каждого колоночного семейства и позволяет запомнить значение моментально. Технически это хеш-таблица (hashmap) с возможностью одновременного доступа (concurrent access) на основе структуры данных, называемой “списками с пропусками” (skip list). Журнал закрепления один на всё пространство ключей и сохраняется на диске. Журнал представляет собой последовательность операций модификации. Так же он разбивается на части при достижении определённого размера. Такая организация позволяет сделать скорость записи ограниченной скоростью последовательной записи на жесткий диск и при этом гарантировать долговечность данных (data durability). Журнал закрепления в случае аварийного останова узла читается при старте сервиса кассандры и восстанавливает все таблицы в памяти. Получается, что скорость упирается во время последовательной записи на диск, а у современных жёстких дисков это порядка 100МБ/с. По этой причине журнал закрепления советуют вынести на отдельный дисковый носитель.

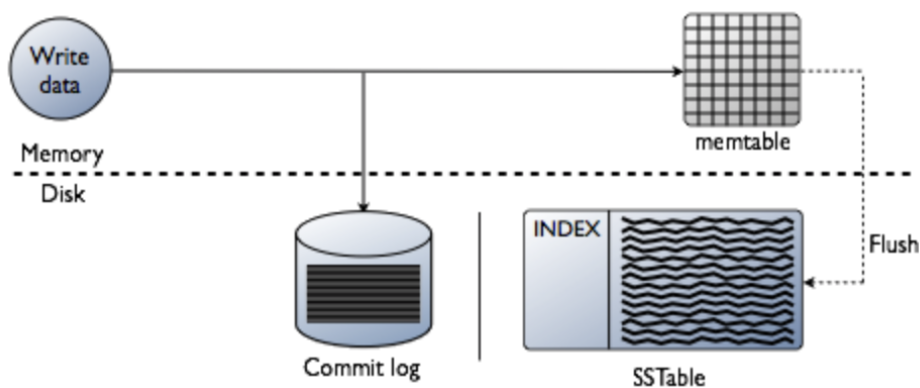


Рис. 3: Схема записи в Cassandra

## 6 Защита данных в распределенных системах

### 6.1 Распределенные вычислительные среды

Распределённая обработка данных - методика выполнения прикладных программ группой систем. При этом пользователь получает возможность работать с сетевыми службами и прикладными процессами, расположенными в нескольких взаимосвязанных абонентских системах. (Sergeeva)

**Распределенная обработка информации в среде клиент-сервер. Концепция распределенной вычислительной среды Distributed Computing Environment (DCE). Распределенные базы данных в сетях ЭВМ**

Компьютер (или программу), управляющий ресурсом, называют сервером этого ресурса (файл-сервер, сервер базы данных, вычислительный сервер...). Клиент и сервер какого-либо ресурса могут находиться как в рамках одной вычислительной системы, так и на различных компьютерах, связанных сетью. Основной принцип технологии "клиент-сервер" заключается в разделении функций приложения на три группы:

- ввод и отображение данных (взаимодействие с пользователем);
- прикладные функции, характерные для данной предметной области;
- функции управления ресурсами (файловой системой, базой данных и т.д.)

Поэтому, в любом приложении можно выделить следующие компоненты:

- компонент представления данных
- прикладной компонент
- компонент управления ресурсом

Связь между компонентами осуществляется по определенным правилам, которые называют "протокол взаимодействия". Каждый из компонентов приложения при этом может работать на выделенном сервере (узле) или разделять ресурсы сервера с другими компонентами приложения. В связи с этим можно выделить следующие модели приложений:

- двухзвенная модель (модель «клиент-сервер»)
- трехзвенная модель (модель сервера приложений)
- многозвенная модель

**Двухзвенная модель** позволяет распределить различным образом три компонента приложения между двумя узлами. **Трехзвенная модель** предполагает выделение для каждого из трех компонентов приложения свой сервер. **Многозвенная модель** позволяет отдельным компонентам использовать ресурсы нескольких серверов, например, распределенные базы данных. Компанией Gartner Group, специализирующейся в области исследования информационных технологий, предложена следующая классификация двухзвенных моделей взаимодействия клиент-сервер (**dce**)

Появление сетей ЭВМ позволило наряду с централизованными создавать и распределенные базы данных. **Распределенная база данных** состоит из нескольких, возможно, пересекающихся или даже дублирующих друг друга частей, хранимых в различных ЭВМ вычислительной сети. Однако пользователь распределенной базы данных не обязан знать, каким образом ее компоненты размещены в узлах сети, и представляет себе эту базу данных как единое целое. Работа с такой базой данных осуществляется с помощью *системы управления распределенной базой данных* (СУРБД).

## 6.2 Угрозы безопасности распределенных СУБД

**Угрозы доступности, целостности и конфиденциальности данных. Механизмы противодействия**

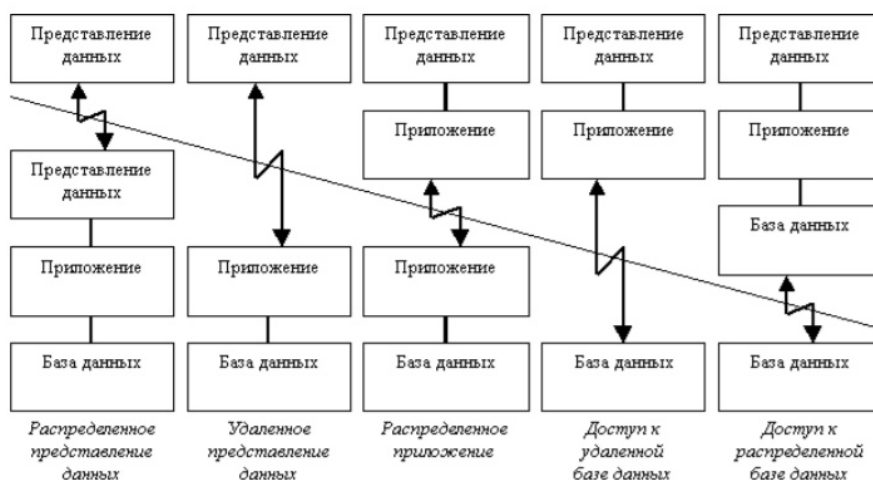


Рис. 4: Классификация двухзвенных моделей

### Современный подход к информационной безопасности

Под информационной безопасностью понимается защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов, а также организационных мер, с целью недопущения причинения вреда владельцам этой информации или поддерживающей ее инфраструктуре.

При построении системы защиты должен учитываться комплексный подход в обеспечении безопасности информации. Он подразумевает использование защитных механизмов на всех этапах жизненного цикла системы, от ее проектирования и до вывода из эксплуатации, и совместное решение целого спектра вопросов, начиная от физической защиты объектов ИС, с применением интеллектуальной системы контроля доступа, и заканчивая вопросами поддержки нормального функционирования ИС в критических ситуациях.

Проектирование системы безопасности информации (СБИ) осуществляется совместно с проектированием самой информационной системы. При внесении любых изменений в структуру ИС, это должно найти адекватное отражение и в системе защиты.

При разработке систем информационной безопасности необходимо учитывать передовые тенденции развития информационных технологий, к каким в настоящее время относятся интрасети (Интранет - Intranet). Характерными чертами данных сетей является то, что они основываются на технологии клиент/сервер, имеют в своем составе разнородные корпоративные информационные системы и пользуются внешними сервисами, базовым для которых является протокол TCP/IP, а также предоставляет аналогичные сервисы вовне. Центральным элементом интрасетей является WEB-сервис, поэтому чрезвычайно важным является вопрос обеспечения защищенности этого сервиса.

### Разработка политики безопасности

Первым шагом на пути построения СБИ является разработка политики безопасности ИС. Под политикой безопасности следует понимать утвержденный высшим должностным лицом организации, в интересах которой разрабатывается ИС и система защиты, документ, с указанием организационных и технических мероприятий, направленных на защиту информации, и поддерживающей



ее инфраструктуры.

В данном документе должны найти обязательное отражение основные принципы безопасности информации, такие как многоуровневая защита и разнообразие средств и методов защиты, минимизация привилегий, разделение полномочий, невозможность обхода средств защиты и т.п.

### **Построение модели нарушителя**

После разработки политики безопасности производится анализ угроз ИС, возможных каналов утечки информации и построение на этой основе модели потенциального нарушителя.

Согласно предлагаемой модели, в качестве нарушителя может выступать как отдельное физическое лицо, так и специальные программы, содержащие в себе некие деструктивные элементы - разрушающие программные компоненты (РПК).

Под объектом защиты в данной модели понимается материальный носитель защищаемой информации, а также сама информация, доступ к которым определен режимом разграничения доступа, реализуемым системой защиты, а также поддерживающая инфраструктура.

Предполагается, что по отношению к ИС нарушитель может быть двух типов: внутренним или внешним. При этом внутренний нарушитель выступает в качестве законного пользователя системы или лица из числа обслуживающего персонала или администрации ИС, а внешний является лицом, не подпадающим ни под одну из указанных категорий. РПК, в свою очередь, может быть отнесено к категории внутреннего нарушителя.

Возможные угрозы нарушителя напрямую зависят от его типа. Возможности внутреннего нарушителя ограничены установленными правилами разграничения доступа, внутриобъектовым режимом и его функциональными обязанностями. Возможности РПК в ИС намного шире и определяются работоспособностью ПО, в котором они заложены, а также наличием в системе средств активного аудита и мониторинга.

### **Проектирование СБИ**

Следующим шагом после разработки модели нарушителя является проектирование СБИ. Согласно принципу многоуровневой защиты и разнообразия средств и методов защиты, можно выделить следующие самостоятельные системы в составе СБИ (при этом необходимо учитывать, что все они интегрированы и находятся в тесной взаимосвязи):

- Система контроля доступа на объекты и в помещения ИС
- Система защиты информации в ИС от НСД
- Средства защиты от РПК
- Средства поддержания доступности информации в ИС

### **Система защиты информации в ИС от НСД**

Данная система может быть реализована как встроенными средствами защиты сетевых операционных систем и систем управления базами данных (СУБД), так и дополнительными средствами. Стоит лишь отметить, что при построении системы защиты от НСД необходимо, по возможности, избегать дублирования многих функций, с тем, чтобы СБИ не страдала избыточностью, что в конечном итоге скажется как на удобстве работы пользователей и их желании выполнять все предписания системы защиты, так и на управляемости самой СБИ.

В состав указанной системы также должны входить:

- средства контроля, управления и идентификации при удаленном доступе
- средства управления доступом и идентификации в рамках ИС
- средства экранирования ИС от открытых сетей, а также разноуровневых сетей внутри данной ИС друг от друга
- средства управления, анализа и аудита СБИ в рамках сетевых конфигураций

### **Средства контроля, управления и идентификации при удаленном доступе к ИС**

Указанная категория средств предназначена для осуществления процедуры контроля подключения к ИС удаленных пользователей, а также для управления их доступом и осуществления идентификации. Данная проблема возникает в связи со структурой интрасетей, когда удаленные пользователи получают доступ к ресурсам корпоративной ИС по выделенным, либо коммутируемым каналам связи. В этом случае существует реальная вероятность несанкционированного подключения нарушителя к линии связи, с активным или пассивным прослушиванием сети и выдачей себя за зарегистрированного пользователя ИС. В целях недопущения подобного целесообразно применение методов с использованием одноразовых паролей и единого входа в сеть

Принцип систем с одноразовыми паролями основан на однократном использовании пароля для процедуры идентификации в ИС, в результате чего перехват его нарушителем становится бессмысленным. Идентификация и аутентификация пользователя осуществляется сервером безопасности (аутентификации), входящим в состав ИС.

Концепция единого входа в сеть предоставляет существенное удобство для пользователей, так как при подключении к ИС им достаточно только один раз доказать свою подлинность. Кроме этого, применение этой концепции способствует усилению информационной безопасности, ввиду того, что в сети отсутствует открытая передача аутентификационной информации.

### **Средства управления доступом и идентификации в рамках ИС**

Учитывая территориальную разнесенность современных ИС и использование технологии клиент/сервер, целесообразно выделение функции проверки подлинности в виде отдельного сервера безопасности (аутентификации). Услугами данного сервера должны пользоваться все другие серверы и пользователи ИС.

Сервер безопасности может быть реализован в виде одного или нескольких серверов, функционирующих на физически защищенных компьютерах. Серверы должны содержать репозиторий субъектов ИС и их секретные ключи.

При построении сервера безопасности возможны два пути:

- Сервер безопасности с центральным хранением данных репозитория
- Сервер безопасности с децентрализованным хранением данных репозитория

Однако централизованное хранение является нецелесообразным по следующим причинам:

- сильная зависимость от готовности сервера
- возможность расширения или комбинирования сетей в процессе развития ИС

Дополнительной причиной децентрализации сервера безопасности является объединение сетей при развитии ИС. Возможна ситуация, когда две до того независимые сети, имеющие каждая в своем составе отдельный сервер безопасности, объединяются. В этом случае один из серверов должен быть уничтожен, а все определенные в нем данные по авторизации переданы на другой сервер. Если же связь между двумя сетями устанавливается временно, то необходимо наличие нескольких серверов безопасности. В противном случае, один сервер должен будет производить постоянные, двойные определения то для одной, то для другой сети. Для того, чтобы избежать этого, необходимо наличие нескольких серверов безопасности.

### **Средства экранирования ИС**

Средства экранирования используются для подключения ИС к открытым сетям или развязки разноуровневых сетей, т.е. сетей, обрабатывающих информацию с различным грифом секретности. Концепция систем типа Firewall (брандмауер, межсетевой экран) была разработана для снижения риска нелегального доступа к закрытой информации при подключении частных сетей (в том числе ЛВС) к сетям общего пользования. Межсетевой экран представляет собой программно-аппаратный комплекс, размещенный на стыке двух сетей и реализующий следующие три функции:

- обеспечение обмена данными между сетями только через указанную систему
- фильтрация трафика обмена
- предотвращение возможности проникновения в сам экран

В этом случае обеспечивается эффективная блокировка внешнего трафика частной сети и жесткий контроль за ним. Кроме того экраны могут осуществлять разграничение доступа между различными сегментами одной корпоративной сети, а также контроль за информационными потоками, направленными во вне, обеспечивая тем самым необходимый режим конфиденциальности.

Применение экранов также позволяет существенно уменьшить уязвимость внутренних сервисов безопасности, так как нарушителю необходимо вначале преодолеть защитные механизмы самого экрана, где они сконфигурированы особенно тщательно.

Существующие в настоящее время экраны могут быть условно разделены на следующие четыре типа:

- экраны с фильтрацией пакетов (packet-filtering firewall)
- плюзы сеансового уровня (circuit-level gateway)
- плюзы прикладного уровня (application-level gateway)
- экраны экспертного уровня (stateful inspection firewall)

Однако лишь некоторые экраны могут быть отнесены только к одной из указанных категорий. При этом необходимо отметить, что экраны экспертного уровня обеспечивают один из самых высоких на сегодняшний день уровней безопасности интрасетей.

### **Средства управления, анализа и аудита**

Средства аудита занимают свое особое положение в ряду средств обеспечения безопасности информации, заключающееся в том, что все действия нарушителя по преодолению средств защиты фиксируются, позволяя тем самым вовремя обнаружить попытку несанкционированного входа

в ИС. Причем, учитывая принцип многоуровневой защиты, нарушителю придется преодолевать несколько защитных рубежей, что будет обязательно отмечено в регистрационном протоколе. В случае если указанная процедура выполняется в режиме реального времени, администратором безопасности могут быть своевременно предприняты соответствующие меры по предотвращению незаконного вторжения на одном из следующих уровнях защиты.

Кроме средств аудита часть программных продуктов также позволяет осуществлять оценку системы безопасности сети, имитируя все известные способы, применяемые нарушителями для проникновения в интрасети, и тем самым, обнаруживая в системе защиты слабые места. Данные программные продукты не только выявляют уязвимые места, но и определяют действия, которые необходимо предпринять для ликвидации пробелов в сетевой системе безопасности. Администратору остается лишь выбрать способы их устранения.

### **Средства резервного копирования**

Резервное копирование программ и данных необходимо проводить с целью минимизации потерь в случае отказов оборудования, либо сбоев в программном обеспечении ИС. Данная задача наиболее сложна именно в интрасетях с их распределенными ресурсами и неоднородностью, в которых работают компьютеры под управлением различных операционных систем. Учитывая клиент/серверный характер интрасетей функцию резервного копирования целесообразно также выделить в виде отдельного сервера (сервера архива).

Распространение клиент/серверного подхода на процедуру резервного копирования информации и данных имеет ряд преимуществ по сравнению с традиционными методами. Они выражаются в следующем:

- Администраторы рабочих групп освобождаются от необходимости согласования действий и самой процедуры создания локальных резервных копий
- Единообразие процедуры создания резервных копий в ИС
- Возможность мониторинга процесса резервирования и диагностики возникших проблем

Одним из способов обеспечения высокой доступности информации является создание резервных копий с возможностью ее хранения в двух местах: один экземпляр хранится поблизости от оригинала, а другой в удаленном безопасном месте.

### **Безопасность систем управления базами данных**

Составной частью информационной безопасности ИС является безопасность систем управления базами данных (СУБД). Учитывая, что СУБД является ключевым элементом современной ИС, можно отметить, что для них важны все три аспекта информационной безопасности: конфиденциальность, целостность и доступность.

В СУБД для идентификации и проверки подлинности применяются либо соответствующие механизмы операционной системы, либо специальный SQL-оператор.

### **Обеспечение конфиденциальности данных**

В СУБД, как правило, используется произвольное управление доступом, когда владелец объекта передает права доступа к нему (привилегии) по своему усмотрению. При этом привилегии в СУБД можно подразделить на две категории: привилегии безопасности и привилегии доступа.

Привилегии безопасности всегда выделяются конкретному пользователю и позволяют выполнять административные действия.

Привилегии доступа определяют права доступа субъектов к определенным объектам.

Специфическим механизмом управления доступом в СУБД являются представления. Они позволяют сделать видимыми для субъектов только те столбцы базовых таблиц, доступ к которым предоставлен субъектам администратором базы.

### **Поддержание целостности**

Целостность данных не менее важна, чем конфиденциальность, ввиду того, что для баз данных, как и для ИС в целом, главными врагами являются не внешние нарушители, а ошибки оборудования, программ, администраторов и пользователей системы.

С точки зрения пользователей СУБД, основными средствами поддержания целостности данных являются ограничения и правила.

Ограничения могут относиться как к таблицам, так и к отдельным столбцам. Они накладываются владельцами таблицы и оказывают влияние на все операции с данными.

Правила позволяют вызывать выполнение заданных действий при определенных изменениях базы данных. В отличие от ограничений, являющихся лишь средствами контроля простых условий, правила позволяют создавать сколь угодно сложные соотношения между различными элементами базы данных.

### **Обеспечение доступности данных**

Доступность данных подразумевает обеспечение информационной системы средствами поддержания высокой доступности. Поддержание высокой доступности позволяет свести к минимуму возможные сбои аппаратного обеспечения, в частности носителей информации, а также ошибки обслуживающего персонала и программного обеспечения. В качестве мер поддержания высокой доступности может быть названа кластеризация сервера баз данных (выделение нескольких компьютеров, выполняющих общее приложение), а также тиражирование данных (хранение базы данных в различных местах).

### **Угрозы СУБД**

СУБД отличаются от других компонентов ИС специфичными угрозами, и главным их источником является сама природа баз данных. Известно, что основным средством общения с СУБД выступает язык SQL, являющийся мощным инструментом манипулирования данными. С его помощью, используя механизм правил, могут быть созданы сложные, трудно поддающиеся анализу цепочки действий, позволяющие не явным образом передавать право на выполнение определенных процедур тем, кто не имеет на это полномочий.

В качестве примера можно привести несколько угроз, возникающих при использовании языка SQL: получение информации путем логических выводов, агрегирование данных, покушение на высокую доступность.

Методы борьбы против получения информации путем логических выводов состоят в тщательном проектировании модели данных, иерархии привилегий и видимых пользователям представлений.

Агрегирование данных состоит в получении новой информации путем комбинирования данных, полученным официальным путем. Причем информация, содержащаяся в скомбинированных данных, может иметь гриф более высокий, чем первичная информация.

Методом борьбы с агрегированием может быть тщательное проектирование модели данных и максимально допустимое ограничение доступа пользователей к информации.

Покушение на высокую доступность может быть реализовано, если пользователю-нарушителю доступны все возможности языка SQL. При этом он легко сможет заблокировать работу других пользователей. Поэтому, в целях борьбы с данным видом угроз, рекомендуется запрещать непосредственный SQL-доступ к базе данных, используя для этого серверы приложений.

## 6.3 Распределенная обработка данных

### Понятие распределенной транзакции

Если данные хранятся в одной базе данных, то транзакция к ней рассматривается как локальная. В распределенных базах транзакция, выполнение которой заключается в обновлении данных на нескольких узлах сети, называется глобальной или **распределенной транзакцией**.

Внешне выполнение распределенной транзакции выглядит как обработка транзакции к локальной базе данных. Тем не менее распределенная транзакция включает в себя несколько локальных транзакций, каждая из которых завершается двумя путями — фиксируется или прерывается. Распределенная транзакция фиксируется только в том случае, когда зафиксированы все локальные транзакции, ее составляющие.

### Модель обработки транзакций

В стандарте ANSI/ISO SQL определены модель транзакций и функции операторов COMMIT и ROLLBACK. Стандарт определяет, что транзакция начинается с первого SQL-оператора, инициируемого пользователем или содержащегося в программе. Все последующие SQL-операторы составляют тело транзакции. Транзакция завершается одним из четырех возможных путей:

- оператор COMMIT означает успешное завершение транзакции; его использование делает постоянными изменения, внесенные в базу данных в рамках текущей транзакции
- оператор ROLLBACK прерывает транзакцию, отменяя изменения, сделанные в базе данных в рамках этой транзакции; новая транзакция начинается непосредственно после использования ROLLBACK
- успешное завершение программы, в которой была инициирована текущая транзакция, означает успешное завершение транзакции (как будто был использован оператор COMMIT)
- ошибочное завершение программы прерывает транзакцию (как будто был использован оператор ROLLBACK)

Точки сохранения применяются, как правило, в протяженных транзакциях и позволяют разделить транзакцию на несколько небольших осмысленных фрагментов. Пользователь может зафиксировать работу в любой точке транзакции с тем, чтобы выполнить ее откат к состоянию, соответствующему этой точке.

Откат и фиксация транзакций становятся возможными благодаря журналу транзакций. Он используется следующим образом. Известно, что все операции над реляционной базой данных суть операции над строками таблиц. Следовательно, для обеспечения отката таблиц к предыдущим состояниям достаточно хранить не состояния таблицы, а лишь те ее строки, которые подверглись изменениям.

При выполнении любого оператора SQL, который вносит изменения в базу данных, СУБД автоматически заносит очередную запись в журнал транзакций. Запись состоит из двух компонентов: первый - это состояние строки до внесения изменений, второй - ее же состояние после внесения изменений. Только после записи в журнал транзакций СУБД действительно вносит изменения в базу данных. Если после данного оператора SQL был выполнен оператор COMMIT, то в журнале транзакций делается отметка о завершении текущей транзакции. Если же после оператора SQL следовал оператор ROLLBACK, то СУБД просматривает журнал транзакций и отыскивает записи, отражающие состояние измененных строк до внесения изменений. Используя их, СУБД восстанавливает те строки в таблицах базы данных, которые были изменены текущей транзакцией, - таким образом аннулируются все изменения в базе данных.

### **Мониторы обработки транзакций**

Мониторы обработки транзакций (Transaction Processing Monitor - TPM), или, проще, мониторы транзакций - программные системы (которые относят к категории middleware, то есть к посредническому или промежуточному программному обеспечению), обеспечивающие эффективное управление информационно-вычислительными ресурсами в распределенной системе. Они представляют собой гибкую, открытую среду для разработки и управления мобильными приложениями, ориентированными на оперативную обработку распределенных транзакций. В числе важнейших характеристик TPM - масштабируемость, поддержка функциональной полноты и целостности приложений, достижение максимальной производительности обработки данных при невысоких стоимостных показателях, поддержка целостности данных в гетерогенной среде. TPM опираются на трехзвенную модель "клиент-сервер" (модель сервера приложений или AS-модель), описанную в Разделе 2. Естественно, что все преимущества модели отражаются и на программных системах, построенных на ее основе.

На современном рынке мониторов транзакций основными "действующими лицами" являются такие системы, как ACMS (DEC), CICS (IBM), TOP END (NCR), PATHWAY (Tandem), ENCINA (Transarc), TUXEDO System (USL). Несмотря на принципиальное сходство, конкретные TPM отличаются рядом характеристик, причем различия часто вытекают как из специфики операционной системы, в которой реализован и функционирует TPM.

### **Корпоративная среда обработки транзакций**

TPM на базе UNIX опирается на фундаментальное понятие - корпоративную среду обработки транзакций (Enterprise Transaction Processing - ETP). Архитектура ETP - это три ряда компьютеров:

- Ряд 1: Персональные станции (Personal Workstations);
- Ряд 2: Компьютеры под управлением ОС UNIX (UNIX Transaction Processing Servers - UPTS);
- Ряд 3: Mainframe-системы (Proprietary Transaction Processing Servers - PTPS) или компьютеры под управлением UNIX с RISC-архитектурой процессоров;

Компьютеры **ряда 1**, функционирующие под управлением DOS, MS Windows, OS/2, UNIX, используются в качестве рабочих мест конечных пользователей. Характерная черта ETP - отсутствие ограничений на модели компьютеров, составляющих этот ряд. Однако, как правило, ряд 1

состоит из компьютеров на базе процессоров Intel 486/Pentium под управлением MS Windows (MS Windows фактически стала стандартом оконного графического интерфейса для большинства категорий пользователей и стандартом операционной среды для подавляющего числа прикладных программ и систем).

**Ряд 2** составляют компьютеры среднего класса под управлением ОС UNIX, на которых функционирует ядро ТРМ и, как правило, реляционные СУБД (Oracle, Informix, Ingres), выступающие в качестве менеджера ресурсов. Кроме того, на них же может быть установлен шлюз к ТРМ в операционной среде мэйнфрейма (как правило, разработчики ТРМ на базе UNIX предусматривают в конфигурации своих систем шлюз к наиболее популярной такой системе - IBM CICS).

**Ряд 3** представлен мэйнфреймами или RISC-компьютерами под управлением UNIX. О мэйнфреймах мы говорим в тех ситуациях, когда исторически сложилось так, что в организации они существуют уже долгое время, берут на себя большую часть всего объема обработки транзакций, концентрируют огромные вычислительные ресурсы и содержат большие массивы данных (то есть речь идет об унаследованных системах). Если этого "тяжелого наследия" нет, то можно смело использовать в качестве компьютеров ряда 3 RISC-серверы, сегодня приближающиеся по производительности к мэйнфреймам.

Таким образом, среда обработки транзакций формируется из набора разнородных компьютеров (и соответствующих ОС), ранжируемых от персональных компьютеров до мэйнфрейм-систем. ТРМ на базе UNIX представляет собой своего рода "клей который связывает вместе компьютеры трех рядов в открытую унифицированную среду обработки транзакций.

Ключом к интеграции систем, функционирующих на компьютерах различных рядов, является специализированный интерфейс прикладного программирования ATMI (Application Transaction Manager Interface), обеспечивающий:

- для ряда 1 - формирование и передачу запросов от клиентов к серверам, выполняющимся на компьютерах ряда 2
- для ряда 2 - обработку запросов, поступающих от компьютера ряда 1 (в том числе и с обращением к менеджеру ресурсов), и, по необходимости, формирование и направление запросов к серверам, выполняющимся на компьютерах ряда 3
- для ряда 3 - обработку запросов, поступающих от серверов ряда 2

Стоит отметить, что подобное представление о корпоративной среде обработки транзакций не является абстракцией. Сегодня многие организации приходят именно к такой, "трехуровневой" архитектуре информационных систем (с той оговоркой, что наличие ряда 3 вызвано историческими причинами - мэйнфреймы использовались первоначально и сразу от них отказаться невозможно).

## 6.4 Протоколы фиксации

### Протоколы фиксации

В локальной системе базы данных для принятия транзакции диспетчер транзакций должен только передать решение о фиксации диспетчеру восстановления. Однако в распределенной системе диспетчер транзакций должен передать решение о фиксации всем серверам в различных сайтах,



где выполняется транзакция, и обеспечить единообразное выполнение решения. Когда обработка завершается на каждом сайте, она достигает состояния частично подтвержденной транзакции и ожидает, пока все другие транзакции достигнут их частично подтвержденных состояний. Когда он получает сообщение о том, что все сайты готовы к фиксации, он начинает фиксировать. В распределенной системе либо все сайты фиксируют, либо ни один из них не делает.

Различные протоколы распределенной фиксации:

- Однофазный коммит
- Двухфазный коммит
- Трехфазный коммит

### **Распределенная однофазная фиксация**

Распределенная однофазная фиксация – это самый простой протокол фиксации. Давайте рассмотрим, что есть контролирующий сайт и несколько подчиненных сайтов, где выполняется транзакция. Шаги в распределенном коммите:

- После того, как каждое ведомое устройство локально завершило свою транзакцию, оно отправляет сообщение «ГОТОВО» на контролирующий сайт
- Подчиненные ожидают сообщения «Подтвердить» или «Прервать» с контролирующего сайта. Это время ожидания называется окном уязвимости
- Когда контролирующий сайт получает сообщение «СДЕЛАНО» от каждого ведомого, он принимает решение о фиксации или отмене. Это называется точкой фиксации. Затем он отправляет это сообщение всем рабам
- При получении этого сообщения ведомое устройство либо фиксирует, либо прерывает работу, а затем отправляет подтверждающее сообщение на контролирующий сайт

После того, как каждое ведомое устройство локально завершило свою транзакцию, оно отправляет сообщение «ГОТОВО» на контролирующий сайт.

Подчиненные ожидают сообщения «Подтвердить» или «Прервать» с контролирующего сайта. Это время ожидания называется окном уязвимости.

Когда контролирующий сайт получает сообщение «СДЕЛАНО» от каждого ведомого, он принимает решение о фиксации или отмене. Это называется точкой фиксации. Затем он отправляет это сообщение всем рабам.

При получении этого сообщения ведомое устройство либо фиксирует, либо прерывает работу, а затем отправляет подтверждающее сообщение на контролирующий сайт.

**Распределенная двухфазная фиксация** Распределенная двухфазная фиксация снижает уязвимость однофазных протоколов фиксации. Шаги, выполняемые на двух этапах:

#### **Этап 1**

- После того, как каждое ведомое устройство локально завершило свою транзакцию, оно отправляет сообщение «ГОТОВО» на контролирующий сайт. Когда контролирующий сайт получил сообщение «ГОТОВО» от всех подчиненных, он отправляет сообщение «Подготовить» подчиненным

- Рабы голосуют за то, хотят ли они по-прежнему совершать или нет. Если ведомый хочет зафиксировать, он отправляет сообщение «Готово»
- Раб, который не хочет коммитить, отправляет сообщение «Не готов». Это может произойти, если ведомое устройство имеет конфликтующие параллельные транзакции или истекло время ожидания

После того, как каждое ведомое устройство локально завершило свою транзакцию, оно отправляет сообщение «ГОТОВО» на контролирующий сайт. Когда контролирующий сайт получил сообщение «ГОТОВО» от всех подчиненных, он отправляет сообщение «Подготовить» подчиненным.

Рабы голосуют за то, хотят ли они по-прежнему совершать или нет. Если ведомый хочет зафиксировать, он отправляет сообщение «Готово».

Раб, который не хочет коммитить, отправляет сообщение «Не готов». Это может произойти, если ведомое устройство имеет конфликтующие параллельные транзакции или истекло время ожидания.

## Этап 2

- После того, как контролирующий сайт получил сообщение «Готово» от всех ведомых –
  - Контролирующий сайт отправляет сообщение «Global Commit» подчиненным
  - Подчиненные устройства применяют транзакцию и отправляют сообщение «Подтвердить АСК» на контролирующий сайт
  - Когда контролирующий сайт получает сообщение «Подтвердить АСК» от всех ведомых устройств, он считает транзакцию подтвержденной
- После того, как контролирующий сайт получил первое сообщение «Не готов» от любого ведомого –
  - Контролирующий сайт отправляет сообщение «Global Abort» подчиненным
  - Слэйвы отменяют транзакцию и отправляют сообщение «Abort АСК» на контролирующий сайт
  - Когда контролирующий сайт получает сообщение «Abort АСК» от всех ведомых устройств, он считает транзакцию отмененной

**Распределенная трехфазная фиксация** Шаги в распределенной трехфазной фиксации следующие:

- Этап 1: Шаги такие же, как при распределенной двухфазной фиксации
- Этап 2: Подготовьтесь к фиксации
  - Контролирующий сайт выдает широковещательное сообщение «Ввод подготовленного состояния»
  - Ведомые сайты голосуют «ОК» в ответ
- Фиксация / Отмена

Этапы аналогичны двухфазной фиксации, за исключением того, что сообщение «Подтвердить АСК» / «Прервать АСК» не требуется

## Защищенные протоколы фиксации

### Обработка распределенных транзакций в базах данных с многоуровневой секретностью (MLS)

Известно, что в MLS/DBMS не ко всем данным, содержащимся в базе данных, доступ осуществляется одинаково. Однако современные СУБД, как правило, не имеют адекватных средств диагностики и механизма определения того, что пользователь имеет возможность доступа только к тем данным, которые являются релевантными. Таким образом, MLS/DBMS отличается от соответствующих DBMS, по крайней мере, следующими двумя особенностями:

- каждый элемент данных в базе данных связан с уровнем доступа
- доступ пользователя к данным должен контролироваться релевантностью для данного пользователя

Разработка сервиса MLS/DBMS в современных компьютерных системах представляет много проблем. До настоящего времени внедрение многоуровневого разграничения доступа в операционную систему представляет собой значительные трудности. Решение этой проблемы в виде аббревиатуры обозначается TCB. Хотя в разрешении вопросов TCB для удаленных пользователей в MLS/DBMS вводятся компромиссы, остается много проблем, которые требуется разрешать. Наиболее очевидная проблема состоит в том, что вопросы классификации в СУБД значительно сложнее, чем в файловых системах и могут быть сложнее реализованы. Другая проблема состоит в том, что для классификации данных, содержащих контекстные представления, временные параметры, их композицию, необходимы унифицированные базы данных.

## 6.5 Тиражирование данных

**Тиражирование данных** - это асинхронный перенос изменений объектов исходной базы данных (source database) в базы данных, принадлежащие к различным узлам распределенной системы. Функции тиражирования данных возложены на специальный компонент СУБД - сервер тиражирования данных, называемый репликатором (replicator), задача которого состоит в обеспечении идентичности данных в принимающих базах данных (target database) данным в исходной БД.

### Обзор средств тиражирования данных

На практике установка тиражируемой системы сводится к чисто административным действиям, для выполнения которых необходимо получить ответы на четыре вопроса: **Что** тиражировать? **Где** тиражировать? **Когда** тиражировать? **Как разрешать** предполагаемые конфликты?

**Что тиражировать?** Как и любая другая методология, тиражирование имеет собственную терминологию. Краеугольным камнем тиражирования является понятие согласованного распределенного набора данных (consistent distributed data set - CDDS). Фактически, это тот самый набор данных в базе (или база данных целиком), идентичность которого на всех узлах, вовлеченных в процесс тиражирования, и поддерживает репликатор. Здесь и далее мы будем говорить об узлах распределенной системы, хотя участвовать в тиражировании могут и базы данных, расположенные на одном узле.

CDDS может быть представлен следующими конфигурациями данных:

- Вся база данных
- Избранные объекты базы данных: таблицы или представления
- Вертикальные проекции объектов БД: избранные столбцы таблиц и/или представлений
- Горизонтальные подмножества объектов: избранные записи из таблиц и/или представлений
- Сочетание наборов 2-4

### **Где тиражировать?**

Следующий основополагающий элемент схемы тиражирования - это путь переноса изменений (data propagation path - DPP) из каждой тиражируемой базы данных в другие БД. Гибкость тиражирования в значительной степени обеспечивается богатством выбора способа передачи данных между узлами распределенной системы.

Практика эксплуатации распределенных систем подсказала следующие схемы тиражирования данных, реализуемые репликатором:

- Центр-филиалы изменения в БД филиалов переносятся в центральную БД, и /или наоборот
- Равноправное, несколько БД разделяют общий набор изменяемых и тиражируемых данных
- Каскадное, изменения в одной БД переносятся в другую БД, откуда в свою очередь в третью БД и т. д., эта схема позволяет оптимизировать баланс загрузки серверов баз данных, расположенных на различных узлах
- Через шлюзы изменения в базе данных могут переноситься в БД другой СУБД
- Различные комбинации всех перечисленных выше схем

### **Когда тиражировать?**

После определения тиражируемого набора данных и маршрута переноса изменений остается определить лишь момент инициации репликационного сервера. Как уже говорилось раньше, элементарным изменением, вызывающим реакцию репликатора, является транзакция, но тиражировать каждую транзакцию по одиночке было бы не всегда удобным. Например, было бы трудно зафиксировать состояние в принимающей базе данных на определенный час. Стремясь быть максимально гибким, репликатор предоставляет следующие возможности:

- тиражирование начинается после завершения определенного числа транзакций, в том числе и после каждой транзакции
- тиражирование происходит через равные промежутки или к определенному моменту времени
- процесс тиражирования контролируется вручную администратором системы или созданным пользователем монитором тиражирования

### Как разрешать конфликты?

Конфликты, возникающие в некоторых ситуациях, например, при встречном тиражировании или при восстановлении базы данных с помощью репликатора из реплицированной копии, можно отнести к разряду планируемых проблем. Репликатор при необходимости самостоятельно обнаруживает противоречия в тиражируемых данных и предоставляет разрешение конфликта администратору (противоречивые данные обязательно регистрируются в журнале), либо делает это автоматически. Возможны следующие варианты:

- разрешение конфликта в пользу более раннего или более позднего изменения
- разрешение конфликта в пользу наивысшего приоритета тиражируемой записи

### Эффективные алгоритмы тиражирования

Алгоритмы тиражирования:

- Алгоритм восстановления данных при тиражировании
- Алгоритм создания копии при тиражировании данных

Более подробно об алгоритмах тиражирования можно почитать тут ([https://www.hse.ru/data/2010/08/04/121Lyadova\\_Strelkov.pdf](https://www.hse.ru/data/2010/08/04/121Lyadova_Strelkov.pdf))

### Сравнение подходов к тиражированию БД

## 6.6 Интеграция БД и Internet

### Современные тенденции

### Обзор существующих технологий

### Вопросы безопасности: угрозы и методы противодействия

### Перспективы развития

## 7 Безопасность в статистических БД

Инфы про статистические базы данных на русском языке мало и большая часть бредовая. Гуглите statistical database. Все источники будут на английском, переведено специально для вас. Источников несколько **ComputerSecurity2008 IntroBD2014**, под конец была найдена статья, **SDB1989** в которой есть вся собранная инфа.

## 7.1 Общие сведения

. Определение статистической БД. Классификация статистических БД. Характеристики статистических БД.

Статистической (в приведенном здесь контексте) называется база данных, в которой допускаются запросы с обобщением данных (суммированием, вычислением среднего значения и т.д.), но не допускаются запросы по отношению к элементарным данным. Например, в статистической базе данных разрешается выдача запроса "Какова средняя зарплата программистов? тогда как выдача запроса "Какова зарплата программиста Мэри?" запрещена. Проблема статистических баз данных заключается в том, что иногда с помощью логических заключений на основе выполнения разрешенных запросов можно вывести ответ, который прямо может быть получен только с помощью запрещенного запроса. "Обобщенные значения содержат следы исходной информации, и она может быть восстановлена злоумышленником после соответствующей обработки этих обобщенных значений. Такой процесс называется логическим выводом конфиденциальной информации". Практически для любой статистической базы данных всегда может быть определен общий трекер (в отличие от множества индивидуальных трекеров). Общий трекер (general tracker) — это логическое выражение, которое может быть использовано для поиска ответа на любой запрещенный запрос, т.е. запрос, включающий недопустимое логическое выражение. (В противоположность этому индивидуальный трекер работает только на основе запросов, включающих конкретные запрещенные выражения.) Требуется поддерживать баланс между репрезентативностью данных и конфиденциальностью отдельных записей.

## 7.2 Классификация

Классифицирует по следующим признакам:

- Чисто статистическая база данных - Обычная база данных со статистическим доступом

этот тип базы данных хранит только статистические данные. Примером может служить база данных переписи населения. этот тип базы данных содержит отдельные записи. Кроме того, база данных поддерживает набор статистических пользователей, которым разрешены только статистические запросы. Для этих последних пользователей совокупная статистика, основанная на базовых необработанных данных, генерируется в ответ на запрос пользователя или может быть предварительно вычислена и сохранена как часть базы данных.

- Оффлайн-Онлайн

В онлайн-SDB существует прямое взаимодействие пользователя с данными в режиме реального времени через терминал. В автономном SDB пользователь не контролирует обработку данных и не знает, когда выполняется его запрос данных. В этом режиме методы защиты, отслеживающие профили пользователей, становятся более громоздкими. Компромиссные методы, требующие большого количества запросов (например, метод компромисса на основе регрессии, см. Раздел 7), также усложняются при работе в автономном режиме.

- Статическая-Динамический

Статическая база данных-это такая база данных, которая никогда не меняется после ее создания. Большинство баз данных переписи являются статическими. Всякий раз, когда создается

новая версия базы данных, эта новая версия считается другой статической базой данных. В отличие от этого, динамические базы данных могут изменяться непрерывно. Эта особенность может значительно усложнить проблему безопасности, поскольку частые выпуски новых версий могут позволить ищейкам использовать различия между версиями способами, которые трудно предвидеть. Методы возмущения данных могут не подходить для динамических СДБ, так как усилия по преобразованию исходного СДБ в возмущенный могут стать непомерными.

- **Централизованный-Децентрализованный**

В централизованном SDB есть одна база данных. В децентрализованном (распределенном) SDB перегруженные подмножества базы данных хранятся на различных узлах, Соединенных коммуникационной сетью. Распределенная база данных может быть полностью реплицирована, частично реплицирована или секционирована. Проблема безопасности распределенного SDB является более сложной, чем проблема централизованного SDB из-за необходимости дублировать на каждом узле накладные расходы по контролю безопасности, а также трудности интеграции профилей пользователей. Выделенная-общая компьютерная система в выделенной SDB компьютерной системе используется исключительно для обслуживания приложений SDB. В общей системе приложения SDB работают на одной аппаратной системе с другими приложениями (возможно, с использованием различных баз данных). Общую среду защитить сложнее, так как другие приложения могут вмешиваться в защищаемые данные непосредственно через операционную систему, минуя механизм безопасности SDB.

### 7.3 Угрозы статистических БД

Об безопасности в статистических БД Деннинг [16.6]

"методы нарушения защиты данных просты и не связаны с большими расходами. Поэтому требование обеспечения полной секретности конфиденциальной информации несовместимо с требованием возможности вычисления точных статистических показателей для произвольных подмножеств данных в базе. По крайней мере одно из этих требований должно быть снято прежде, чем можно будет поверить в гарантии обеспечения секретности.

То есть существует мнение, что нельзя нормально обезопасить СБД.

Основная проблема СБД – проблема вывода. В общих чертах, проблема вывода для SDB может быть сформулирована следующим образом. Характеристическая функция  $C$  определяет подмножество записей (строк) в базе данных. Запрос, использующий  $C$ , предоставляет статистику по выбранному подмножеству. Если подмножество достаточно мало, возможно, даже одна запись, спрашивающий может быть в состоянии сделать вывод о характеристиках одного человека или небольшой группы. Даже для больших подмножеств характер или структура данных могут быть такими, что несанкционированная информация может быть выпущена. Для злоумышленника, который пытается достать индивидуальные данные задача состоит в том, чтобы сделать общий трекер. Нужно придумать такую последовательность запросов, чтобы вывести индивидуальную информацию. Суть в том, что можно набрать несколько запросов и проделать операции над ними там, чтобы деанонить записи.

Например для статичной СБД можно сделать такое

запрос1: выдать  $a1 + a2 + a3$ , запрос2: выдать  $a1 + a2$ . запрос1 - запрос2 =  $a3$ .

Для динамической онлайн СБД Мы хотим достать зарплату Мэри. Знаем, что ей 20 лет. Записываем в базу много левых записей с возрастом = 20 лет и нулевой зарплатой. Делаем запрос с минимальной агрегацией людей с возрастом 20 лет. Таким образом можно узнать возможную зп Мэри. Чем больше исходных знаний есть о Мэри, тем точнее получим данные. Также не стоит забывать что речь идет о БД. Поэтому статистическая БД наследует все опасности обычных БД.

## 7.4 Защита в статистических БД

Разделяют четыре общих подхода защиты статистических БД:

- концептуальный;
- ограничение запросов;
- возмущение данных;
- возмущение вывода;

На рисунке 5 изображена схема 3 подходов.

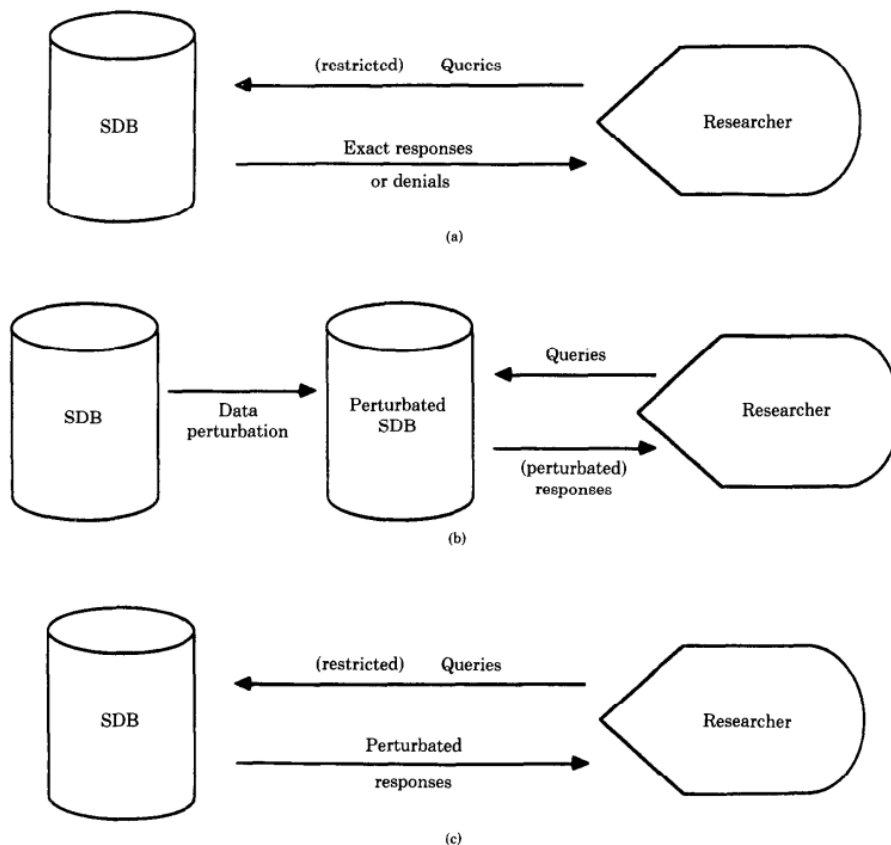


Рис. 5: Схемы безопасности СДБ



**Концептуальный** Основная проблема в том, что вся реляционная алгебра позволяет выводить индивидуальные данные. Концептуальный подход предлагает заменить классическую систему реляционной БД работающую с индивидуальными данными. Основной подход: Partitioning of the data base – Записи хранятся не отдельно, а агрегировано и обезличено. Судя по-всему похоже на microaggregation. Microaggregation – есть исходные данные, выделим несколько записей, посчитаем для них средние значения, заменим значения записей полученным средним, повторить для остальных записей в исходных данных

Еще один способ – решетчатая модель. Агрегация данных по разным признакам на разном уровне детализации.

Ну и естественно не забываем про классические способы. Access Restriction - пусть вы доктор, тогда вам можно всё. А исследователям и прочим анонам даём только некоторые записи или даже готовые стат.результаты по данным (агрегация)

**Ограничение запросов** Query Set Restriction – Ограничение на минимальный размер выдаваемой выборки.

Limiting intersection of query sets – Метод защиты блокирует такие запросы которые приводят к выводу данных через пересечение множеств запросов. Сохранение исторических сведений о результатах выполнения запросов и отклонение любых запросов, использующих значительное количество исходных данных, обработанных предыдущим запросом. Auditing - ведём логи, ловим негодяев и всяких подознительных

**Возмущение данных** Data Perturbation – добавим небольшой, случайный шум. Тогда точные данные вроде как и будут уничтожены, но можно заиграться и исказить репрезентативность

Случайное добавление дополнительных строк к основному набору данных, обрабатываемому запросом. Также предлагается организовать "обмен данными"("data swapping"), т.е. обмен значениями атрибутов между кортежами, осуществляемый таким образом, чтобы поддерживалась лишь статистическая точность. При этом даже если злоумышленнику удастся идентифицировать отдельное значение (например, некоторое значение зарплаты), то у него не будет способа узнать, какому именно кортежу (в нашем примере — сотруднику) оно принадлежит. Сложность этого подхода заключается в необходимости отыскать множество тех записей, между которыми можно будет организовать обмен значениями соответствующим образом. Подобные затруднения имеют место и при использовании большинства других методов.

**Возмущение вывода** Output Perturbation – как предыдущее, но преобразовывать будем результат каждого запроса Random Sampling – сделать так, чтобы один и тот же запрос давал каждый раз разные наборы записей Использование для ответов на запросы только случайных наборов исходных данных

**Критерии безопасности** Как было сказано гарантированной безопасности в СДБ не добиться. Поэтому делают оценку важности деанонимизированных данных и статистической точности (из-за наших всех действий для защиты данных)

Security – сферическая вероятность раскрыть (в том числе частично) запись в сбд Для каждого разрешенного агрегирующего запроса оценивается критерий безопасности. На основе количества

инфы в базе можно подсчитать сколько тех или иных запросов нужно сделать для деанонимизации. На основе этого рассчитывается минимальная выборка для таких запросов.

Consistency – оценивается консистентность данных для методов возмущения данных. Оценивается степень возмущения данных. Создаем агрегирующий запрос и замеряем его изменения после внесенных возмущений. Robustness – оценка зависимости между возмущением и конкретной записью. Было бы круто чтобы возмущение не было зависимо от данных, но нужно каким-то образом сохранить ее статистические свойства.

Costs – Назначаем каждому запросу конкретную цену. Пользователю даем начальную сумму на которую он может делать запросы, такую чтобы он не смог вывести данные. Выглядит больше как метод, а не критерий.

## 8 Распознавание вторжений в БД

### 8.1 Основные понятия

**Обнаружение вторжений** (применительно к БД) – процесс выявления действий, которые способны нарушить конфиденциальность, целостность и доступность информации, хранимой в базе данных (БД).

**Система обнаружения вторжений (СОВ)** [согласно ФСТЭК] – программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Применение систем обнаружения вторжения относится к реактивным мерам (то есть к таким мерам, которые используются уже после того, как произошел инцидент) для противодействия активности злоумышленника в тех случаях, когда злоумышленник преодолел все проактивные меры. Поэтому обычно системы обнаружения вторжений являются *вторичным фактором защиты в общей системе защиты* и предназначены для обнаружения и регистрации уже произошедших событий, а также оповещение персонала при срабатывании определенных правил.

Если классифицировать методы обнаружения вторжения, используемые в системах обнаружения вторжений (СОВ), то можно выделить три типа (согласно классификации, предложенной Стефаном Аксельсоном [IDSClassification]):

- синтаксические методы (или методы поиска злоупотреблений, англ. misuse detection). К таким методам обычно относятся методы, которые основываются на обнаружения вторжений путём сравнения SQL-запросов с шаблонами недопустимых синтаксических конструкций.
- методы обнаружения аномалий (англ. anomaly detection). Такие методы, наоборот, в отличие от первого типа, подразумевают создание шаблонов нормального поведения пользователя и последующее сравнение этих шаблонов с действиями, выполняемыми пользователями во время работы с БД.
- смешанные методы, представляющие собой композицию первых двух

## 8.2 Системы распознавания вторжений

Системы обнаружения вторжения (англ. Intrusion Detection System, IDS) и системы предотвращения вторжений (англ. Intrusion Prevention System, IPS) обычно рассматриваются вместе, причем часто под термином система предотвращения вторжений подразумевается расширение систем обнаружения вторжений, так как IPS системы также должны обладать возможностью обнаружения вторжений. Иначе говоря, IPS системы являются активными IDS системами.

В IDS системах, система также ответственна за реализацию ответных мер на нарушения: блокировка соединения, настройки межсетевого экрана и прочее. Таким образом,

**Система обнаружения и предотвращения вторжений (IPS/IDS)** (применительно к БД) – это программное или программно-техническое средство, предназначенное для выявления фактов неавторизованного доступа и предотвращения попыток несанкционированного доступа к БД.

### 8.2.1 Типы моделей систем распознавания вторжений (ID-систем)

Существует множество способов классификации COB, которые не являются однозначными или обязательными. Следует рассмотреть наиболее известные и используемые классификации, которые характеризуют систему по:

- По способу мониторинга
- По способу анализа
- По скорости реакции
- По классу защиты

**По способу мониторинга.**

- **Сетевая COB (англ. Network-based IDS, NIDS)** – система, которая занимается проверкой сетевого трафика с концентратора или коммутатора и анализируя сетевые пакеты.
- **Узловая COB (англ. Host-based IDS, HIDS)** – система, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников.
- **Основанная на прикладных протоколах COB (англ. Application-based IDS, APIDS)** – система, в которой ведется наблюдение за специализированными прикладными протоколами и анализ соответствующих данных. Например, на веб-сервере с SQL базой данных COB будет отслеживать содержимое SQL команд, передаваемых на сервер.
- **Гибридная COB** – система, которая является композицией нескольких видов систем обнаружения вторжений.

**По способу анализа.** О данной классификации уже говорилось ранее. Она строится по методу анализа событий, полученных из источника информации, и методу принятия решения, что происходит проникновение. Способами анализа являются **обнаружение злоупотреблений** и **обнаружение аномалий**.

**По скорости реакции.** Определяют два типа СОВ по времени между получением информации из источника и ее анализом и принятием решения. В зависимости от задержки во времени, СОВ разделяются на:

- **с пакетным режимом (англ. interval-based).** В таких системах реакция происходит через определенные интервалы времени, а информационный поток от точек мониторинга до инструментов анализа не является непрерывным.
- **непрерывные (англ. real-time).** В таких системах обрабатывается непрерывный поток информации от источников. При этом таких тип является преобладающей типом в сетевых СОВ, которые получают информацию из потока сетевого трафика.

**По классу защиты.** Для каждой сертифицированной в России СОВ присваивается некоторый класс защиты согласно классификации ФСТЭК и выполненным требованиям для определенного профиля защиты (ПЗ). Всего существует 6 классов, где самый низкий класс - шестой, а самый высокий - первый.

Согласно ФСТЭК СОВ разделяются на [IDSFSTEK]:

- **СОВ с 6 классом защиты:** применяются в информационных системах персональных данных 3 и 4 классов.
- **СОВ с 5 классом защиты:** применяются в информационных системах персональных данных 2 класса.
- **СОВ с 4 классом защиты:** применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.
- **СОВ с 3, 2 или 1 классом защиты:** применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

## 8.2.2 Общая структура ID-систем

**Архитектура СОВ.** Основными архитектурными компонентами СОВ являются:

1. **Host** – система, на которой выполняется ПО СОВ.
2. **Target** – система, за которой наблюдает СОВ.

Первоначально многие СОВ выполнялись на тех же системах, которые они защищали. Основная причина этого была в том, что большинство систем было mainframe, и стоимость выполнения СОВ на отдельном компьютере была очень большой. Это создавало проблему с точки зрения безопасности, так как любой атакующий, который успешно атаковал целевую систему, мог в качестве одной из компонент атаки просто запретить функционирование СОВ.

Но с появлением рабочих станций и персональных компьютеров в большинстве архитектур СОВ предполагается выполнение СОВ на отдельной системе, тем самым разделяя системы Host и Target. Это улучшает безопасность функционирования СОВ, так как в этом случае проще спрятать существование СОВ от атакующих.

### Компоненты современных СОВ:

- сенсор, который отслеживает события в сети или системе;
- анализатор событий, обнаруженных сенсорами;
- компонента принятия решения.

### Способы управления СОВ:

- **Централизованное управление.** При централизованных стратегиях управления весь мониторинг, обнаружение и отчетность управляются непосредственно с единого "поста". В этом случае существует единственная консоль СОВ, которая связана со всеми сенсорами, расположенными в сети.
- **Частично распределенное управление.** Мониторинг и определение управляются с локально управляемого узла, с иерархической отчетностью в одно или более центральных расположений.
- **Полностью распределенное управление.** Мониторинг и определение выполняются с использованием подхода, основанного на агентах, когда решения об ответе делаются в точке анализа.

При этом в сети должны поддерживаться следующие связи:

- связи для передачи отчетов СОВ. Эти связи создаются между сенсорами как сетевого мониторинга, так и мониторинга хоста, и центральной консолью СОВ;
- связи для мониторинга хостов и сетей;
- связи для выполнения ответов СОВ.

### 8.2.3 Шаблоны классов пользователей

Рассматривать шаблоны классов пользователей имеет смысл только в контексте СОВ, применяющих методы обнаружения аномалий, так как именно они строят и используют такие шаблоны поведения пользователей. Таким образом, детекторы аномалий определяют необычное поведение на хосте или в сети. Они предполагают, что атаки отличаются от некоторой нормальной деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов или сетевых соединений. Эти профили создаются, исходя из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной.

Метрики и технологии, используемые при определении аномалий, включают:

- определение допустимого порога. В этом случае основные атрибуты поведения пользователя и системы выражаются в количественных терминах. Для каждого атрибута определяется некоторый уровень, который устанавливается как допустимый. Такие атрибуты поведения могут

определять число файлов, доступных пользователю в данный период времени, число неудачных попыток входа в систему, количество времени ЦП, используемое процессом и т.п. Данный уровень может быть статическим или эвристическим — например, может определяться изменением анализируемых значений.

- статистические метрики: параметрические, при которых предполагается, что распределение атрибутов профиля соответствует конкретному образцу, и непараметрические, при которых распределение атрибутов профиля является "обучаемым" исходя из набора значений истории, которые наблюдались за определенный период времени.
- метрики, основанные на правилах, которые аналогичны непараметрическим статистическим метрикам в том, что наблюдаемые данные определяют допустимые используемые образцы, но отличаются от них в том, что эти образцы специфицированы как правила, а не как численные характеристики.
- другие метрики, включая нейросети, генетические алгоритмы и модели иммунных систем.

#### **Преимущества определения аномалий:**

- IDS, основанные на определении аномалий, обнаруживают неожиданное поведение и, таким образом, имеют возможность определить симптомы атак без знания конкретных деталей атаки.
- Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур для детекторов злоупотреблений.

#### **Недостатки определения аномалий:**

- Подходы определения аномалий обычно создают большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности.
- Подходы определения аномалий часто требуют некоторого этапа обучения системы, во время которого определяются характеристики нормального поведения.

#### **8.2.4 Модели известных атак**

- Необычные запросы и команды администрирования SQL сервера, часто употребляемые взломщиками (DROP, CREATE и т.д.)
- Незаконные операции DELETE, UPDATE и INSERT
- Запросы, содержащие id администратора
- Обращение к служебным таблицам и скрытым данным
- Запросы, всегда возвращающие TRUE
- Попытка обнулить поля с паролем
- Внедрение в запросе OR, сравнения констант и другое

### 8.3 Экспертные ИД-системы

Технологию построения экспертных систем часто называют инженерией знаний. Как правило, этот процесс требует специфической формы взаимодействия создателя экспертной системы, которого называют инженером знаний, и одного или нескольких экспертов в некоторой предметной области. Инженер знаний «извлекает» из экспертов процедуры, стратегии, эмпирические правила, которые они используют при решении задач, и встраивает эти знания в экспертную систему. В результате появляется компьютерная программа, которая решает задачи во многом так же, как эксперты – люди (**ExpertSystems**).

В экспертных системах могут использоваться импликационные правила (Если [условие] то [действие]). Например:

- ЕСЛИ с одного узла за время  $T$  поступает  $N$  пакетов, ТО записать в лог факт: происходит DoS атака (факт  $A$ )
- Если наблюдается более чем  $N$  фактов  $A$ , ТО записать в лог факт: происходит DDoS атака

#### 8.3.1 Метрики

- **Показатель активности** – величина, при превышении которой активность подсистемы оценивается как быстро прогрессирующая. В общем случае используется для обнаружения аномалий, связанных с резким ускорением в работе. Пример: среднее число записей аудита, обрабатываемых для элемента защищаемой системы в единицу времени.
- **Распределение активности в записях аудита** – распределение во всех типах активности в актуальных записях аудита. Здесь под активностью понимается любое действие в системе, например, доступ к файлам, операции ввода-вывода.
- **Измерение категорий** – распределение определенной активности в категории <sup>12</sup>. Например, относительная частота количества регистраций в системе (логинов) из каждого физического места нахождения. Предпочтения в использовании программного обеспечения системы (почтовые службы, компиляторы, командные интерпретаторы, редакторы и т.д.)
- **Порядковые измерения** – используется для оценки активности, поступающей в виде цифровых значений. Например, количество операций ввода-вывода, инициируемых каждым пользователем. Порядковые измерения вычисляют общую числовую статистику значений определенной активности, в то время как измерение категорий подсчитывает количество активностей.

#### 8.3.2 Статистические модели

При обнаружении аномалий с использованием профайла в основном применяют статистические методы оценки. Процесс обнаружения происходит следующим образом: текущие значения измерений профайла сравнивают с сохраненными значениями. Результат сравнения - показатель аномальности в измерении. Общий показатель аномальности в простейшем случае может вычисляться при помощи некоторой общей функции от значений показателя аномалии в каждом измерении профайла.

---

<sup>12</sup>Здесь под *категорией* понимается группа подсистем, объединенных по некоему общему принципу

Например, пусть  $M_1, M_2, \dots, M_n$  – измерения профайла, а  $S_1, S_2, \dots, S_n$  – соответственно представляют собой значения аномалии каждого из измерений. Чем больше число  $S_i$ , тем больше аномалии в  $i$ -ом показателе. Объединяющая функция может быть взвешенной суммой их квадратов:

$$a_1 s_1^2 + a_2 s_2^2 + \dots + a_n s_n^2 > 0, \quad (1)$$

где  $a_i$  – отражает относительный вес метрики  $M_i$ .

Параметры  $M_1, M_2, \dots, M_n$  могут быть зависимыми друг от друга. В таком случае, объединяющая функция будет более сложной.

### 8.3.3 Профили

Одним из способов формирования «образа» нормального поведения системы состоит в накоплении измерений значения параметров оценки в специальной структуре данных. Эта структура данных называется *профайлом*.

Основные требования, предъявляемые к структуре профайла:

- Минимальный конечный размер
- Быстрое выполнение операции обновления

### 8.3.4 Примеры ID-систем

**GreenSQL** (APIDS система) – межсетевой экран, функционирующий как прокси-сервер между веб-приложением и SQL сервером. То есть приложение устанавливает соединения к БД не напрямую, а через сервер GreenSQL. GreenSQL анализирует SQL запросы на предмет аномальных запросов, и в случае нормального запроса (то есть если степень риска запроса мала) перенаправляет его на внутренний сервер БД.

GreenSQL поддерживает следующие режимы работы:

- **Режим симуляции (англ. Simulation Mode)** – пассивная система обнаружения атак (IDS). Протоколирует SQL запросы, выдает предупреждения на консоль управления.
- **Блокировка подозрительных команд (англ. Blocking Suspicious Commands/Risk Based)** – активная СОВ. Атаки не только обнаруживаются, но и блокируются (IPS) в соответствии с установленными правилами, указывающими на аномальность запроса.
- **Активная защита от неизвестных запросов (англ. Database Firewall)** – блокирование всех неизвестных запросов.
- **Режим обучения (англ. Learning mode)** – предназначен для прогона и настройки правил в «чистой» среде, что позволяет сформировать белый список и предотвратить в последствии ложные срабатывания анализатора запросов.

Особенности GreenSQL:

- Поддержка ряда СУБД: Microsoft SQL 2000/2005/2008, MySQL 4.x/5.x, PostgreSQL 7.x/8.x.
- Является кросс-платформенной. Среди официально поддерживаемых платформ Microsoft Windows Server 2003/2008, Ubuntu, CentOS. Поддерживаются 32-х и 64-х разрядные системы.



- GreenSQL находит подозрительные запросы, используя ряд методов:
  - Путем определения административных и чувствительных команд SQL. Например: SHOW TABLES, CREATE TABLE, ALTER TABLE.
  - Путем подсчета риска запроса. На это может влиять пустая строка пароля, "or" внутри запроса или выражения SQL, которые всегда возвращают истину (1=1).

**Snort** (NIDS система) – свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом, способная выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP-сетях.

Snort поддерживает следующие режимы работы:

- **Sniffer mode.** В таком режиме программа только считывает сетевые пакеты и выводит их на консоль.
- **Packet Logger Mode.** В режиме логирования пакетов, программа будет регистрировать/логировать пакеты на диске.
- **Network Intrusion Detection System Mode.** В режиме обнаружения вторжений программа будет отслеживать сетевой трафик и анализировать его в соответствии с набором правил, определенным пользователем. Затем программа выполнит определенное действие, основанное на том, что было идентифицировано.

Особенности Snort:

- Возможность написания собственных правил.
- Расширение функциональности с помощью подключения дополнительных модулей.
- Гибкая система оповещения об атаках: Log-файлы, устройства вывода, БД и прочие.

**Suricata** (NIDS система) – свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом. Основана разработчиками, которые трудились над IPS версией Snort, поэтому имеет схожий функционал и обладает полной поддержкой формата правил Snort.

Особенности Suricata:

- Многозадачность.
- Автоматическое определение протокола.
- Высокая производительность, позволяющая обрабатывать трафик до 10Gbit на обычном оборудовании.

**Sagan** (HIDS система) – многопоточная, высокопроизводительная система анализа журналов и мониторинга появления в логах событий, связанных с безопасностью, и реагирования на эти события в режиме реального времени. Система работает в операционных системах Unix.

Sagan также относится к категории систем управления инцидентами и событиями информационной безопасности (англ. Security Information and Log Management, SEIM).

## 8.4 Развитие систем распознавания вторжений

### 8.4.1 Развитие практических аспектов СОВ

Коммерческое использование СОВ находится в стадии формирования. Некоторые коммерческие СОВ получили негативную публичную оценку за большое число ложных срабатываний, неудобные интерфейсы управления и получения отчетов, огромное количество отчетов об атаках, плохое масштабирование и плохую интеграцию с системами сетевого управления. Тем не менее потребность в хороших СОВ возрастает, поэтому с большой вероятностью эти проблемы будут успешно решаться в ближайшее время.

Ожидается, что улучшение качества функционирования СОВ будет осуществляться аналогично антивирусному ПО. Раннее антивирусное ПО создавало большое число ложных тревог при нормальных действиях пользователя и не определяло все известные вирусы. Однако сейчас положение существенно улучшилось, антивирусное ПО стало прозрачным для пользователей и достаточно эффективным.

Более того – очень вероятно, что основные возможности СОВ скоро станут ключевыми в сетевой инфраструктуре (такой как роутеры, мосты и коммутаторы) и в операционных системах. При этом, скорее всего, разработчики СОВ сфокусируют свое внимание на решении проблем, связанных с масштабируемостью и управляемостью СОВ.

Имеются также и другие тенденции, которые, скорее всего, будут влиять на функциональности СОВ следующего поколения. Существует заметное движение в сторону аппаратно-программных (appliance) решений для СОВ. Также вероятно, что в будущем некоторые функции определения соответствия шаблону могут быть реализованы в аппаратуре, что увеличит скорость обработки.

Наконец, механизмы, связанные с управлением рисками в области сетевой безопасности, будут оказывать влияние на требования к СОВ.

### 8.4.2 Развитие теоретических аспектов СОВ

Дальнейшие направления совершенствования связаны с внедрением в теорию и практику СОВ общей теории систем, методов синтеза и анализа информационных систем, конкретного аппарата теории распознавания образов. Эти разделы теории предполагают получение конкретных методов исследования для области систем СОВ.

До настоящего времени не описана СОВ как подсистема информационной системы в терминах общей теории систем. Необходимо обосновать показатель качества СОВ, элементный состав СОВ, ее структуру и взаимосвязи с информационной системой.

В связи с наличием значительного количества факторов различной природы, сложенная работа информационной системы и СОВ имеет вероятностный характер. Вследствие этого актуальным является обоснование вида вероятностных законов конкретных параметров функционирования. Особо следует выделить задачу обоснования функции потерь информационной системы, задаваемую в соответствии с ее целевой функцией на области параметров функционирования системы. При этом целевая функция должна быть определена не только на экспертном уровне, но и в соответствии с совокупностью параметров функционирования всей информационной системы и задачами, возложенными на нее. В таком случае показатель качества СОВ будет определяться как один из параметров, влияющих на целевую функцию, а его допустимые значения – допустимыми значениями функции потерь.

После обоснования законов и функций, реальной задачей является получение оптимальной структуры СОВ в виде совокупности математических операций с помощью формализованных методов. Таким образом, может быть решена задача синтеза структуры СОВ. На основе полученных математических операций можно будет рассчитать зависимости показателей качества функционирования СОВ от параметров ее функционирования, а также от параметров функционирования информационной системы, то есть, будет возможен реальный анализ качества функционирования СОВ.

Сложность применения формализованного аппарата анализа и синтеза информационных систем к СОВ заключается в том, что конкретные реализации информационного комплекса и его подсистемы - СОВ состоят из разнородных элементов, которые могут описываться различными разделами теории (системами массового обслуживания, конечными автоматами, теорией вероятности, теорией распознавания образов и т.д.), то есть, рассматриваемый объект исследования является составным. В результате, математические модели, по-видимому, можно получить только для отдельных составных частей СОВ, что затрудняет анализ и синтез СОВ в целом. Однако, дальнейшая конкретизация применения формализованного аппарата анализа и синтеза позволит оптимизировать СОВ.

На основе изложенного можно сделать вывод о наличии в практической среде значительного опыта решения проблем обнаружения вторжений. Применяемые СОВ в значительной степени основаны на эмпирических схемах процесса обнаружения вторжений. Дальнейшее совершенствование СОВ связано с конкретизацией методов синтеза и анализа сложных систем, теории распознавания образов в применении к СОВ.

## 9 Проектирование безопасности БД

### 9.1 Основные понятия

**Безопасное программное обеспечение** Безопасное программное обеспечение - программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

**Правила безопасности** Политика безопасности — это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации. Только человек, четко осознающий цели организации и условия ее функционирования, может определить, какую информацию необходимо защищать и насколько существенными могут стать потери от несанкционированного распространения, искажения или разрушения информации. После того как политика безопасности определена, должен решаться вопрос о технологии ее реализации в автоматизированном контуре. Для реализации сформулированных в терминах естественного языка правил и норм политики безопасности необходимо использовать (или разработать) некоторую формальную модель, которая допускает эффективное программирование на каком-либо формальном языке. Наибольшее распространение в настоящее время получили две базовые модели безопасности данных: дискреционная и мандатная.

## 9.2 Методология проектирования

### 9.2.1 Отличия в проектировании безопасных ОС и СУБД

Системы управления базами данных (СУБД), как и операционные системы, содержат комбинацию сервисов безопасности, однако, в отличие от ОС, не являются самодостаточными. СУБД используют механизмы и функции ОС. Такая двухуровневость ведет к появлению специфических угроз и требует привлечения соответствующих средств противодействия. Например, базы данных располагаются в файлах или на дисках, управляемых ОС; следовательно, к объектам БД можно обратиться как штатными средствами СУБД, так и с помощью механизмов ОС, получив доступ к файлу или устройству. Подобные возможности должны учитываться в профиле защиты для СУБД. Необходимо реализовать хотя бы один из двух механизмов аутентификации: внешний (аутентификация средствами ОС) или внутренний (аутентификация средствами СУБД). Еще одно проявление упомянутой выше двухуровневости - предположение безопасности базовой конфигурации, состоящее в том, что базовая система ( операционная система, и/или сетевые сервисы безопасности, и/или специальное программное обеспечение) установлены, сконфигурированы и управляются безопасным образом. Аналогичную направленность имеют цели безопасности для среды, предусматривающие, что базовая система должна обеспечить механизмы управления доступом, которые позволят защитить от несанкционированного доступа все связанные с СУБД файлы; кроме того, ОС предоставит средства для изоляции функций безопасности и защиты процессов СУБД. Однако в распределенной информационной системе уровень безопасности может поддерживаться не только средствами базовой ОС, но и архитектурно, путем разнесения компонентов СУБД по узлам сети и использования межсетевых экранов.

### 9.2.2 Основные требования к безопасности СУБД

Можно выделить меры обеспечения безопасности СУБД зависящие и независящие от данных. **Не зависящими** от данных можно назвать следующие требования:

- **Функционирование в доверенной среде.** Под доверенной средой следует понимать инфраструктуру предприятия и ее защитные механизмы, обусловленные политиками безопасности. Таким образом, речь идет о функционировании СУБД в соответствии с правилами безопасности, применяемыми и ко всем прочим системам предприятия.
- **Организация физической безопасности файлов данных.** Требования к физической безопасности файлов данных СУБД в целом не отличаются от требований, применяемых к любым другим файлам пользователей и приложений.
- **Организация безопасной и актуальной настройки СУБД.** Данное требование включает в себя общие задачи обеспечения безопасности, такие как своевременная установка обновлений, отключение неиспользуемых функций или применение эффективной политики паролей.

Следующие требования можно назвать **зависящими** от данных:

- **Безопасность пользовательского ПО.** Сюда можно отнести задачи построения безопасных интерфейсов и механизмов доступа к данным.

- **Безопасная организация и работа с данными.** Вопрос организации данных и управления ими является ключевым в системах хранения информации. В эту область входят задачи организации данных с контролем целостности и другие, специфичные для СУБД проблемы безопасности. Фактически эта задача включает в себя основной объем зависящих от данных уязвимостей и защиты от них.

### 9.2.3 Независимые принципы целостности данных

В работах Кларка и Вильсона определены девять абстрактных теоретических принципов, выполнение которых позволит обеспечить целостность данных:

- **корректность транзакций;** По первому принципу данные могут изменяться только посредством «корректных» транзакций. Прямое (произвольным образом) изменение данных не допускается. В свою очередь корректность транзакций должна быть некоторым способом доказана.
- **авторизация пользователей;** Вторым принципом гласит, что изменение данных может осуществляться только авторизованными пользователями, имеющими определенные привилегии.
- **минимизация привилегий;** Минимальность привилегий подразумевает, что пользователи (в конечном счете, субъекты) должны быть наделены теми и только теми привилегиями, которые минимально необходимы для выполнения тех или иных действий.
- **разграничение функциональных обязанностей;** Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный с точки зрения целостности процесс, необходимо участие различных пользователей. Этим гарантируется, что один пользователь не может выполнить весь процесс целиком (или даже две его стадии) с тем, чтобы нарушить целостность данных.
- **аудит произошедших событий;** Аудит произошедших событий (включая возможность восстановления полной картины происшедшего) является превентивной мерой в отношении потенциальных нарушителей и позволяет восстановить данные в случае их повреждения.
- **объективный контроль;** Принцип объективного контроля также является одним из краеугольных камней политики контроля целостности. Суть данного принципа заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. Очевидно, что нет смысла заботиться о целостности данных, связанных с размещением боевого арсенала, который уже отправлен на переплавку. В связи с этим Кларк и Вильсон указывают на необходимость регулярных проверок, целью которых является выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.
- **управление передачей привилегий;** Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам

безопасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится тяжким бременем и провоцирует попытки обойти ее там, где она мешает «нормальной» работе.

- **эффективное применение механизмов защиты;** В основу восьмого принципа контроля целостности заложен ряд идей, призванных обеспечить эффективное применение имеющихся механизмов обеспечения безопасности. На практике зачастую оказывается, что предусмотренные в системе механизмы безопасности или некорректно используются, или полностью игнорируются системными администраторами.
- **простота использования защитных механизмов;** Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой - наиболее защищенным.

#### 9.2.4 Модель авторизации в System R

Подход к авторизации в System R основан на списках доступа, с возможностью отмены доступа. В System R нет администратора базы данных - суперпользователя в обычном смысле. Любой пользователь может создавать таблицы. Когда пользователь создал таблицу он становится ее суперпользователем. Если он хочет поделиться своей таблицей с другими пользователями, он может использовать команду GRANT для предоставления различных привелегий в этой таблице различным пользователям, таким образом составляя Access List для пользователей, имеющих доступ к таблице, состоящий из UID пользователей.

#### 9.2.5 Архитектура безопасной СУБД

Многоуровневые защищенные архитектуры РСУБД можно разделить на два общих типа, в зависимости от того, осуществляется ли принудительный контроль доступа самой РСУБД или делегируется доверенной операционной системе. Эти два основных типа - это архитектура Вудс-Холла и архитектура TrustedSubjects.

**Архитектура Вудс-Холла** Архитектура Вудс-Холла предполагает, что для доступа к данным используется ненадежная стандартная РСУБД и что доверенный код разрабатывается вокруг этой РСУБД для обеспечения общей безопасной РСУБД. Их можно разделить на две категории: ядерные (kernel) архитектуры и распределенные архитектуры.

**Ядерная(kernel) архитектура** Ядерная архитектура использует надежную операционную систему и несколько копий готовой СУБД, где каждая копия связана с некоторым доверенным интерфейсом. Каждая пара (доверенный интерфейс, СУБД) связана с определенным уровнем безопасности. Доверенная операционная система применяет свою политику полного контроля доступа ко всем доступам СУБД к объектам СУБД. Это гарантирует, что данные с разными уровнями безопасности хранятся отдельно, и что каждая копия СУБД получает доступ к данным, авторизованным для соответствующего уровня безопасности. Последнее возможно, потому что многоуровневая база данных разбита на несколько одноуровневых баз данных, каждая из которых представляет собой фрагмент концептуальной многоуровневой базы данных. Каждый фрагмент хранится в одноуровневом объекте операционной системы (например, в файле), который помечен операционной системой

на соответствующем уровне безопасности, и, таким образом, к нему можно получить доступ только в соответствии с политикой MAC операционной системы.

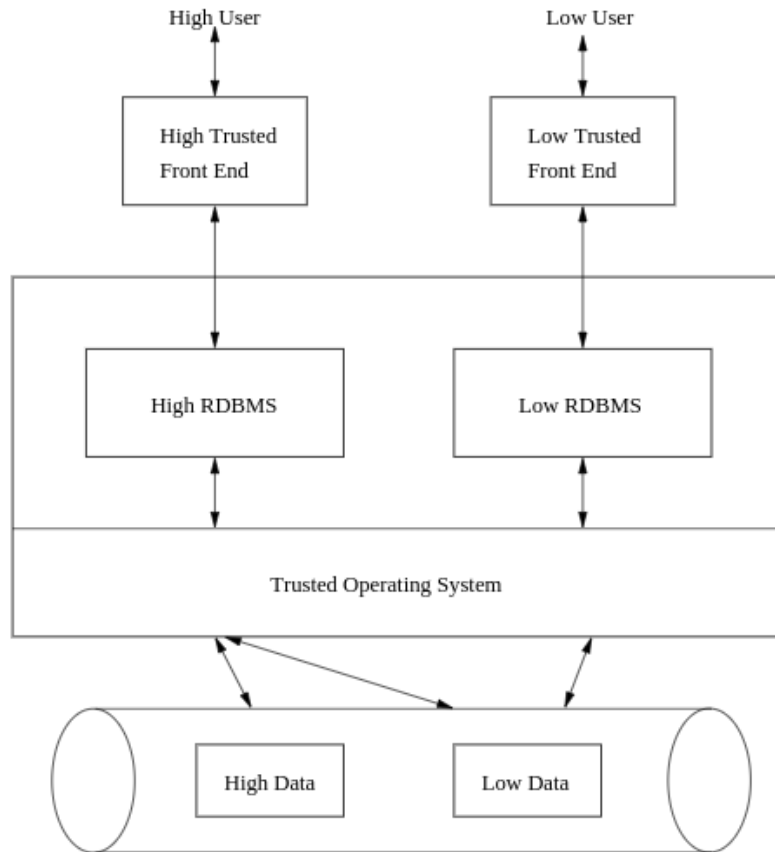


Figure 1: Multilevel secure kernelized RDBMS architecture.

Рис. 6: Ядерная архитектура

На картинке изображена Ядерная архитектура, в которой одна РСУБД связана с уровнем безопасности «Высокий», а другая РСУБД связана с уровнем безопасности «Низкий». РСУБД, связанная с уровнем безопасности «Высокий», имеет доступ как к фрагменту базы данных с высоким уровнем безопасности, так и к фрагменту базы данных с низким уровнем безопасности. А РСУБД, ассоциированная с уровнем безопасности «Низкий», имеет доступ только к фрагменту базы данных с низким уровнем безопасности. Преимущество этой архитектуры заключается в том, что данные на разных уровнях безопасности изолированы. Еще одно преимущество состоит в том, что при условии, что надежная операционная система уже готова, эта архитектура должна минимизировать количество времени и усилий для установки СУБД. Однако эта архитектура приводит к дополнительным накладным расходам, поскольку доверенной операционной системе необходимо разделять

данные на разных уровнях безопасности при добавлении в базу данных, а также может потребоваться совершать трудоемкие операции объединения данных с разных уровней безопасности.

**Распределенные архитектуры** Распределенная (или реплицированная) архитектура - это вариант ядерной архитектуры. Он использует несколько копий доверенного интерфейса и СУБД, каждая из которых связана со своим собственным хранилищем базы данных. В этой архитектурной схеме СУБД на уровне безопасности содержит реплику каждого элемента данных, к которому субъект на уровне может получить доступ. Таким образом, когда данные извлекаются повторно, СУБД извлекает их только из своей собственной базы данных. Еще одно преимущество этой архитектуры состоит в том, что данные физически разделены на отдельные аппаратные базы данных. Однако эта схема приводит к дополнительным накладным расходам, когда данные обновляются, поскольку различные реплики должны быть синхронизированы.

**Архитектура TrustedSubjects** Архитектура TrustedSubjects - это схема, которая содержит надежную СУБД и надежную операционную систему. Согласно этой архитектуре, политика обязательного контроля доступа обеспечивается самой СУБД. Объекты базы данных (например, таблица) хранятся в объектах операционной системы (например, в файле) с наивысшим уровнем безопасности. Таблица базы данных может содержать хранить строки с разными уровнями безопасности. Такие строки различаются на основе их уровня безопасности, который явно сохраняется с каждой строкой. Эта архитектура называется TrustedSubjects, потому что РСУБД имеет привилегию нарушать политику MAC операционной системы при доступе к объектам базы данных. Например, когда пользователь с низким уровнем безопасности запрашивает таблицу базы данных, к объекту операционной системы, в котором хранится эта таблица, оказывается, что это является нарушением MAC-политики операционной системы. Но РСУБД способна возвращать пользователям только те строки, для которых он или она авторизованы в соответствии с политикой MAC. Преимущество этой архитектуры состоит в том, что СУБД имеет доступ ко всем уровням данных в одно и то же время, что сводит к минимуму извлечение и обработку обновлений. Однако эта архитектура приводит к созданию специальной РСУБД, которая требует разработки и проверки большого количества доверенного кода наряду с обычными функциями РСУБД. Недостатком можно считать недостаточный уровень гарантии аппаратной изоляции объектов. Также сложно доказать, что доверенное программное обеспечение, используемое для изоляции объектов (например, потоков данных с разными уровнями безопасности), работает правильно, не допуская потока данных с высоким уровнем безопасности для пользователей с низким уровнем безопасности.



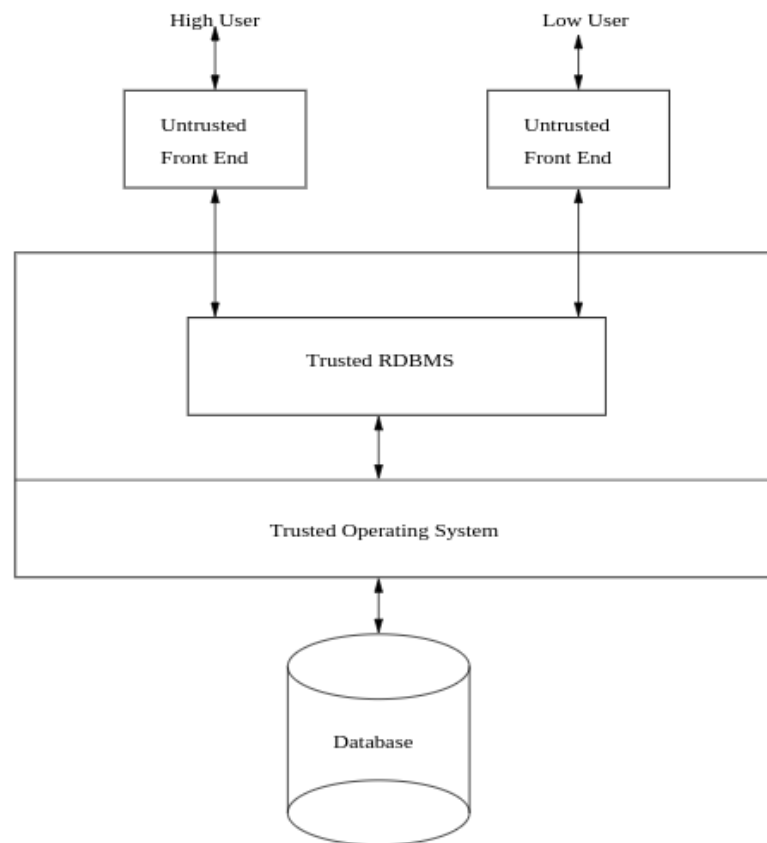


Figure 2: Multilevel secure trusted subject RDBMS architecture.

Рис. 7: архитектура TrustedSubjects

### 9.3 Проектирование безопасных БД

Разработать универсальную защищенную систему баз данных скорее всего нереально. При любом разумном методе измерения уровня защищенности этот уровень является неубывающей функцией от затрат на построение системы защиты. В любом практическом случае, когда существуют ограничения на бюджет системы защиты, существует и некоторый предельный уровень информационной безопасности, который теоретически может быть достигнут.

В настоящее время отсутствует общепринятая методология разработки защищенных автоматизированных информационных систем и, в частности, систем баз данных. В подобных случаях традиционно используется подход, основанный на анализе лучшего мирового опыта решения некоторого класса проблем и формулировании руководящих принципов построения соответствующих систем, концентрирующих накопленный опыт. Именно таким образом для проблемы обеспечения безопасности информационных систем разрабатывался британский стандарт BS 7799 и созданный на его основе международный стандарт ISO 17799.

Анализ наиболее успешных решений в области обеспечения информационной безопасности баз данных позволил сформулировать несколько полезных принципов, которыми можно руководствоваться при проектировании систем защиты:

- **Экономическая оправданность механизмов защиты.** Предписывает использование простейшего из всевозможных вариантов проекта, который обеспечивает достижение желаемой цели. Хотя этот принцип относится ко многим аспектам проектирования систем, он наиболее пригоден при разработке механизмов защиты, так как ошибки проектирования и реализации, которые ведут к неконтролируемым способам доступа к данным, могут быть не замечены в ходе нормального использования системы. Строгое соблюдение этого принципа приводит к применению на практике таких методов, как проверка «строка за строкой» программных средств и физическая проверка аппаратных средств, реализующих механизмы защиты.
- **Открытое проектирование.** Технология систем защиты не должна базироваться на «секретных» алгоритмах. Этот принцип широко используется при проектировании безопасных систем и сетей связи. Высокое качество систем защиты обеспечивается не недостатком знаний у возможных нарушителей, а использованием широко опробованных (как правило, открытых) стандартов и правильной организацией управления ключевой информацией. Использование алгоритмов, основанных на открытых стандартах в области информационной безопасности, повышает степень доверия пользователей к системе защиты и формирует правильную психологическую установку на необходимость внимательности и аккуратности при работе с ключевой информацией.
- **Распределение полномочий между различными субъектами в соответствии с правилами организации.** Состоит в том, что для критически важных приложений целесообразно использовать многокомпонентные схемы доступа к данным. То есть для выполнения соответствующей операции необходимо провести аутентификацию нескольких ее обязательных участников. Физический аналог этого принципа можно наблюдать в конструкциях банковских сейфов, когда для того, чтобы открыть сейф, необходимо наличие двух ключей, которые обычно хранятся у различных людей. Ясно, что механизмы защиты, требующие двух ключей для доступа к информации, являются более устойчивыми, чем механизмы, которые разрешают доступ на основе предъявления единственного ключа. В то же время подобные многокомпонентные процедуры требуют больших затрат и, как правило, более сложных процедур управления ключами (включая хранение резервной копии). При проектировании многокомпонентных схем доступа за образец берется существующая в организации практика. Действительно, переход в автоматизированном контуре на более сложные, чем использовались «в доавтоматизированную эру», технологии может вызвать психологический дискомфорт и различные формы скрытого саботажа системы.
- **Минимально возможные привилегии для пользователей и администраторов.** Предписывает, чтобы каждый пользователь (процесс) системы оперировал с данными, используя наименьший из возможных набор привилегий, необходимых для выполнения конкретной функции. Применение данного принципа нацелено на минимизацию ущерба, который может быть нанесен в случае сбоя, ошибки программного обеспечения или компрометации элементов системы защиты данных. Принцип минимальных привилегий, используемый при созда-

нии пользователей Oracle, — пример реализации этого принципа. Использование точек входа SYSTEM и, особенно, SYS должно быть предметом особого регламента. Хорошей практикой является использование администратором безопасности нескольких точек входа: обычной, с набором привилегий, достаточным для выполнения основных работ, и особой (типа SYSTEM), используемой только при возникновении необходимости выполнения действий, требующих высоких привилегий.

- **Управляемость системы при возникновении отказов и сбоев.** Проектирование информационной системы, реализованной на базе СУБД, должно осуществляться в предположении, что ошибки операционной системы и СУБД, а также сбои аппаратуры неизбежны. При создании системы возможность реализации таких событий должна быть учтена: при проектировании процедур и функций должны быть обработаны все исключительные ситуации, при обработке данных, содержащих конфиденциальную информацию, должны быть минимизированы риски восстановления этих данных по дампам оперативной памяти и содержимому временных файлов и т. п. Также должны быть разработаны документы, регламентирующие действия участников процесса обработки данных (как пользователей, так и обслуживающего персонала) при возникновении нештатных ситуаций. Персонал должен проходить регулярные инструктажи и тренинги по обучению действиям в нештатных ситуациях, с иерархией передачи данных.
- **Психологическая приемлемость работы средств защиты данных.** Взаимодействие людей с системой (и подсистемой защиты) не должно быть сложным. Пользователи должны шаблонно и автоматически применять имеющиеся механизмы защиты. Чрезмерное усложнение механизмов защиты может вызывать их внутреннее неприятие и побуждать к использованию различных форм скрытого саботажа. Осознанное принятие используемых средств и методов обеспечения информационной безопасности и оценка комплекса применяемых мер как необходимых приводит к уменьшению числа ошибок пользователей. В этом случае аномальное поведение потенциального нарушителя становится более заметным и проще устанавливается. Принцип психологической приемлемости является важным при выборе процедур аутентификации и модели управления доступом.

### 9.3.1 Фазы проектирования безопасных БД (по DoD)

Министерство обороны (Department of Defence) предложило методологию проектирования, использования и вывода системы из эксплуатации безопасных информационных систем, в том числе безопасных БД. Стадии жизненного цикла информационной системы, наиболее часто используемые Министерством обороны, показаны на рис. 6.

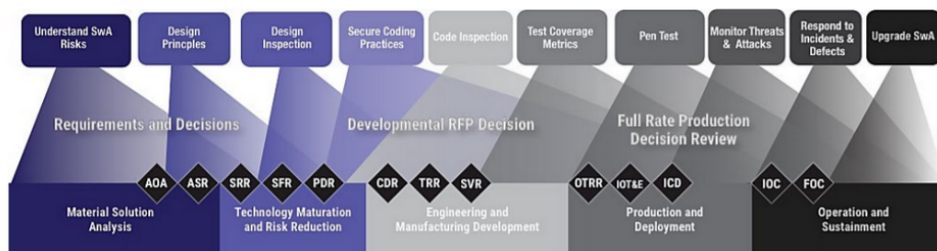


Рис. 8: Стадии жизненного цикла по DoD

Как показано на рис. 6, основная часть жизненного цикла информационной системы включает пять этапов: работа с требованиями, проектирование архитектуры информационной системы, реализация информационной системы, тестирование и введение в эксплуатацию. На этапе требований происходит анализ требований заказчика, формулирование политик безопасности и требований к разрабатываемой информационной системе. На этапе проектирования архитектуры на основе набора требований, представленного в функциональной форме, составляется концептуальная модель системы, на основе концептуальной – логическая, на основе логической – физическая.

### 9.3.2 Предварительный анализ

Анализ требований является одним из первых этапов процесса системного проектирования и в некоторой степени представляет собой интерфейс между внутренними действиями и внешними источниками, предоставляющими входные данные. В процессе анализа требований исследуются, оцениваются и преобразуются внешние входные данные в набор функциональных требований, политик безопасности и требований к производительности, которые будут являться основой для последующего концептуального, логического и физического проектирований. Цель анализа требований – определение требований к системе.

Анализ миссии системы, анализ среды использования системы определяют потребности клиента и формулируют их в терминах, которые могут быть использованы для определения функций системы, требований к производительности или проектных ограничений. Такой анализ определяет функциональные требования к системе, уточняет требования к характеристикам или проектированию. По мере продвижения этой деятельности исходные предположения и выводы сверяются с меняющимися деталями. Обычно это приводит к некоторому изменению исходного мышления заказчика, может даже отражаться на его потребностях, некоторые из которых могут оказаться непрактичными или чрезмерно дорогостоящими.

Результатом анализа требований является набор функциональных определений верхнего уровня и сопутствующих требований к производительности и архитектуре, которые становятся отправной точкой концептуального проектирования. Анализ требований проводится итеративно, цикл анализа требований служит для уточнения требований и инициирования повторной оценки, чтобы определить, насколько жесткими являются требования к элементам системы. Позже подробные характеристики системы сравниваются с установленными требованиями, чтобы убедиться, что они выполняются. На этом этапе обычно мало изменений в требованиях из-за обратной связи проверки, но иногда некоторые незначительные изменения рассматриваются, когда отдача значительна.

### 9.3.3 Требования и политики безопасности

Политика безопасности — это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации. Только человек, четко осознающий цели организации и условия ее функционирования, может определить, какую информацию необходимо защищать и насколько существенными могут стать потери от несанкционированного распространения, искажения или разрушения информации. После того как политика безопасности определена, должен решаться вопрос о технологии ее реализации в автоматизированном контуре. Для реализации сформулированных в терминах естественного языка правил и норм политики безопасности необходимо использовать (или разработать) некоторую формальную модель, которая допускает эффективное программирование на каком-либо формальном языке. Наибольшее распространение в настоящее время получили две базовые модели безопасности данных: дискреционная и мандатная.

Цель формализации политики безопасности для информационной системы — ясное изложение взглядов руководства организации на существо угроз информационной безопасности организации и технологий обеспечения безопасности ее информационных ресурсов. Политика безопасности обычно состоит из двух частей: общих принципов и конкретных правил работы с информационными ресурсами, то есть требований, и, в частности, с базами данных для различных категорий пользователей. Политика безопасности — это всегда некоторый компромисс между желаемым уровнем защищенности ресурсов информационной системы, удобством работы с системой и затратами средств, выделяемых на ее эксплуатацию.

Политика безопасности должна быть оформлена документально на нескольких уровнях управления. На уровне управляющего высшего звена руководства должен быть подготовлен и утвержден документ, в котором определены цели политики безопасности, структура и перечень решаемых задач и ответственные за реализацию политики. Основным документ должен быть детализирован администраторами безопасности информационных систем (управляющими среднего звена) с учетом принципов деятельности организации, соотношения важности целей, и наличия ресурсов. Детальные решения должны включать ясные определения методов защиты технических и информационных ресурсов, а также инструкции, определяющие поведение сотрудников в конкретных ситуациях.

В руководстве по компьютерной безопасности, разработанном национальным институтом стандартов и технологий США (National Institute of Standards and Technology — NIST), рекомендовано включать в описание политики безопасности следующие разделы:

- **Предмет политики.** В разделе должны быть определены цели и причины разработки политики, область ее применения в конкретном фрагменте системы документооборота организации. Должны быть ясно сформулированы задачи, решаемые с использованием информационных систем, которые затрагивает данная политика. При необходимости могут быть сформулированы термины и определения, используемые в остальных разделах.
- **Описание позиции организации.** В этом разделе необходимо ясно описать характер информационных ресурсов организации, перечень допущенных к информационным ресурсам лиц и процессов и порядок получения доступа к информационным ресурсам организации.
- **Применимость.** В разделе может быть уточнен порядок доступа к данным ИС, определены ограничения или технологические цепочки, применяемые при реализации политики безопас-

ности.

- **Роли и обязанности.** В разделе определяются ответственные должностные лица и их обязанности в отношении разработки и внедрения различных элементов политики. Обычно определяются обязанности администратора безопасности данных (отвечает за содержательную сторону предоставления доступа к информационным ресурсам организации), администратора баз данных (определяет техническую реализацию механизмов разграничения доступа), администратора локальной сети, операторов.
- **Соблюдение политики.** В разделе описываются права и обязанности пользователей ИС. Необходимо явное описание и документированное знакомство пользователей с перечнем недопустимых действий при осуществлении доступа к информационным ресурсам организации и наказания за нарушения режимных требований. Должна быть ясно определена технология фиксации фактов нарушения политики безопасности и применения административных мер воздействия к нарушителям.

Для эффективной реализации политика безопасности должна быть понятной всем пользователям информационных систем организации. Возможна подготовка презентаций и проведение семинаров с разъяснением основных положений и практических технологий реализации политики безопасности. Новые сотрудники организации должны быть ознакомлены или обучены конкретным правилам и технологиям доступа к ресурсам ИС, реализованным в соответствии с принятой политикой безопасности. Целесообразно проводить контрольные проверки действий сотрудников с обсуждением результатов.

Эффективное проведение политики безопасности возможно только, если она согласована с существующими приказами и общими задачами организации. Основным способом координации политики безопасности с действующими нормами организации является ее согласование с заинтересованными подразделениями в ходе разработки.

Комплект документов, представляющий основные решения организации по реализации политики безопасности, должен включать:

- документацию, определяющую используемые подходы к оцениванию и управлению рисками для организации в целом и при необходимости конкретных подразделений;
- обоснование принятых решений по выбору средств защиты для рассматриваемой информационной системы;
- формальное описание процедуры определения допустимого уровня остаточного риска;
- директиву, определяющую процедуру проверки режима информационной безопасности и журналов, в которых фиксируются результаты проверки (документы необходимы для осуществления проверки эффективности реализации средств обеспечения информационной безопасности, осуществления их контроля качества и правильности использования);
- документацию, регламентирующую процессы обслуживания и администрирования информационных систем;
- документацию по подготовке периодических проверок по оцениванию и управлению рисками;

- документ «Ведомость соответствия», включающий сведения по организации системы управления информационной безопасностью и регистрации средств управления безопасностью;
- контрмеры для противодействия выявленным рискам.

Успех проведения в жизнь политики безопасности больше зависит от усилий и опытности людей, реализующих политику, чем от сложных программно-технических средств контроля.

### 9.3.4 Концептуальное проектирование

Цель этапа концептуального проектирования – создание концептуальной модели данных исходя из представлений пользователей о предметной области. Для ее достижения выполняется ряд последовательных процедур.

1. **Определение сущностей и их документирование.** Для идентификации сущностей определяются объекты, которые существуют независимо от других. Такие объекты являются сущностями. Каждой сущности присваивается осмысленное имя, понятное пользователям. Имена и описания сущностей заносятся в словарь данных. Если возможно, то устанавливается ожидаемое количество экземпляров каждой сущности.
2. **Определение связей между сущностями и их документирование.** Определяются только те связи между сущностями, которые необходимы для удовлетворения требований к проекту базы данных. Устанавливается тип каждой из них. Выявляется класс принадлежности сущностей. Связям присваиваются осмысленные имена, выраженные глаголами. Развернутое описание каждой связи с указанием ее типа и класса принадлежности сущностей, участвующих в связи, заносится в словарь данных.
3. **Создание ER-модели предметной области.** Для представления сущностей и связей между ними используются ER-диаграммы. На их основе создается единый наглядный образ моделируемой предметной области – ER-модель предметной области.
4. **Определение атрибутов и их документирование.** Выявляются все атрибуты, описывающие сущности созданной ER-модели. Каждому атрибуту присваивается осмысленное имя, понятное пользователям. О каждом атрибуте в словарь данных помещаются следующие сведения:
  - имя атрибута и его описание;
  - тип и размерность значений;
  - значение, принимаемое для атрибута по умолчанию (если такое имеется);
  - может ли атрибут иметь NULL-значения;
  - является ли атрибут составным, и если это так, то из каких простых атрибутов он состоит. Например, атрибут "Ф.И.О. клиента" может состоять из простых атрибутов "Фамилия" "Имя" "Отчество" а может быть простым, содержащим единые значения, как-то "Сидорский Евгений Михайлович". Если пользователь не нуждается в доступе к отдельным элементам "Ф.И.О." то атрибут представляется как простой;
  - является ли атрибут расчетным, и если это так, то как вычисляются его значения.

5. **Определение значений атрибутов и их документирование.** Для каждого атрибута сущности, участвующей в ER-модели, определяется набор допустимых значений и ему присваивается имя. Например, атрибут "Тип счета" может иметь только значения "депозитный" "текущий" "до востребования" "кредит-счет". Обновляются записи словаря данных, относящиеся к атрибутам, – в них заносятся имена наборов значений атрибутов.
6. **Определение первичных ключей для сущностей и их документирование.** На этом шаге руководствуются определением первичного ключа – как атрибута или набора атрибутов сущности, позволяющего уникальным образом идентифицировать ее экземпляры. Сведения о первичных ключах помещаются в словарь данных.
7. **Обсуждение концептуальной модели данных с конечными пользователями.** Концептуальная модель данных представляется ER-моделью с сопроводительной документацией, содержащей описание разработанной модели данных. Если будут обнаружены несоответствия предметной области, то в модель вносятся изменения до тех пор, пока пользователи не подтвердят, что предложенная им модель адекватно отображает их личные представления.

### 9.3.5 Логическое проектирование

Цель этапа логического проектирования – преобразование концептуальной модели на основе выбранной модели данных в логическую модель, не зависящую от особенностей используемой в дальнейшем СУБД для физической реализации базы данных. Для ее достижения выполняются следующие процедуры:

1. **Выбор модели данных.** Чаще всего выбирается реляционная модель данных в связи с наглядностью табличного представления данных и удобства работы с ними.
2. **Определение набора таблиц исходя из ER-модели и их документирование.** Для каждой сущности ER-модели создается таблица. Имя сущности – имя таблицы. Причем каждому атрибуту сущности соответствует столбец таблицы. Правила генерации таблиц из ER-диаграмм опираются на два основных фактора – тип связи и класс принадлежности сущности. Устанавливаются связи между таблицами посредством механизма первичных и внешних ключей. Структуры таблиц и установленные связи между ними документируются.

Изложим правила генерации таблиц из ER-диаграмм, используя пример ER-модели предметной области БАНК, представленной на рис. 7, со следующими наборами атрибутов сущностей предметной области БАНК, представленными на рис. 8.



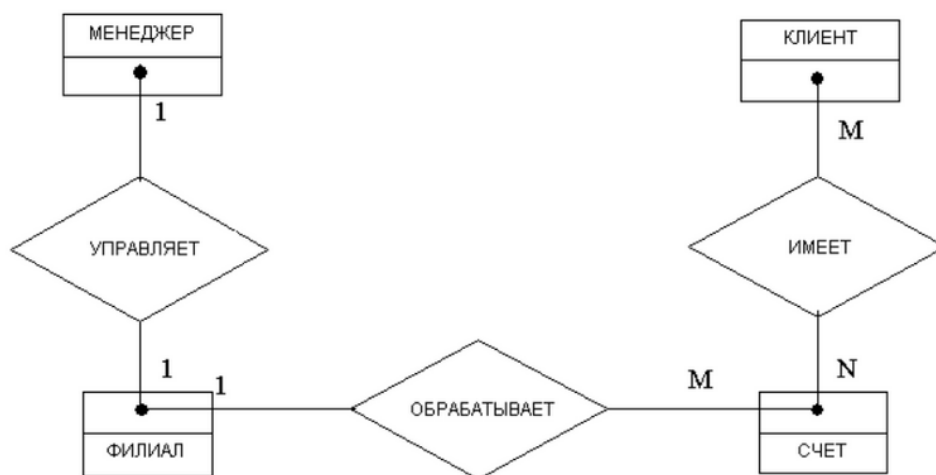


Рис. 9: Пример ER-модели предметной области БАНК

МЕНЕДЖЕР
<b>Номер менеджера (НМ)</b>
Стаж работы (СТАЖ)
Специальность (СПЕЦ)

ФИЛИАЛ
<b>Номер филиала (НФ)</b>
Адрес филиала (АДР_Ф)

СЧЕТ
<b>Номер счета (НС)</b>
Тип счета (ТИП)
Остаток на счете (ОСТ)

КЛИЕНТ
<b>Номер клиента (НК)</b>
Ф.И.О. клиента (ФИО_К)
Социальное положение (СОЦ)
Адрес клиента (АДР_К)

Рис. 10: Наборы атрибутов сущностей предметной области БАНК

Для связи типа 1:1 существуют три отдельных правила формирования предварительных таблиц из ER-диаграмм.

#### Правило 1

Если связь типа 1:1 и класс принадлежности обеих сущностей является обязательным, то необходима только одна таблица. Первичным ключом этой таблицы может быть первичный ключ любой из двух сущностей.

На ER-диаграмме связи 1:1, класс принадлежности сущностей МЕНЕДЖЕР, ФИЛИАЛ является обязательным. Тогда согласно правилу 1 должна быть сгенерирована одна таблица

следующей структуры:

### МЕНЕДЖЕР–ФИЛИАЛ

НМ	СТАЖ	СПЕЦ	НФ	АДР_Ф
----	------	------	----	-------

Первичным ключом этой таблицы может быть и первичный ключ сущности МЕНЕДЖЕР – НМ.

#### Правило 2

Если связь типа 1:1 и класс принадлежности одной сущности является обязательным, а другой – необязательным, то необходимо построить таблицу для каждой сущности. Первичный ключ сущности должен быть первичным ключом соответствующей таблицы. Первичный ключ сущности, для которой класс принадлежности является необязательным, добавляется как атрибут в таблицу для сущности с обязательным классом принадлежности.

Представим, что на ER-диаграмме связи 1:1, изображенной на рис. 7, класс принадлежности сущности МЕНЕДЖЕР будет обязательным, а сущности ФИЛИАЛ – необязательный. Тогда согласно правилу 2 должны быть сгенерированы две таблицы следующей структуры:

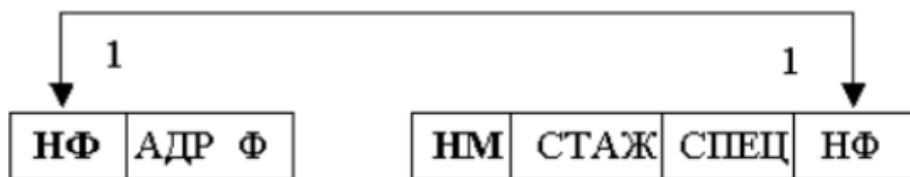
### МЕНЕДЖЕР – ФИЛИАЛ

НМ <input type="checkbox"/>	СТАЖ	СПЕЦ	НФ
-----------------------------	------	------	----

### ФИЛИАЛ

НФ	АДР_Ф
----	-------

Сущность с необязательным классом принадлежности (ФИЛИАЛ) именуется родительской, а с обязательным (МЕНЕДЖЕР) – дочерней. Первичный ключ родительской сущности (НФ), помещаемый в таблицу, представляющую дочернюю сущность, называется внешним ключом родительской сущности. Связь между указанными таблицами устанавливается путем связи первичного и внешнего ключа и имеет вид:



Примечание. Если внешний ключ представляет связь 1:1, то должны быть запрещены его дублирующие значения.

### Правило 3

Если связь типа 1:1 и класс принадлежности обеих сущностей является необязательным, то необходимо построить три таблицы – по одной для каждой сущности и одну для связи. Первичный ключ сущности должен быть первичным ключом соответствующей таблицы. Таблица для связи среди своих атрибутов должна иметь ключи обеих сущностей.

Представим, что на ER-диаграмме связи 1:1, изображенной на рис. 7, класс принадлежности сущностей МЕНЕДЖЕР, ФИЛИАЛ будет необязательным. Тогда согласно правилу 3 должны быть сгенерированы три таблицы следующей структуры:

## МЕНЕДЖЕР

<b>НМ</b>	<b>СТАЖ</b>	<b>СПЕЦ</b>
-----------	-------------	-------------

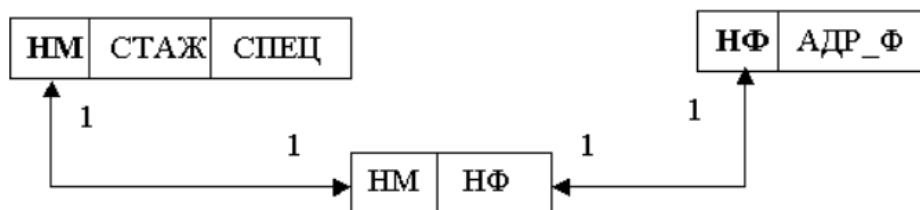
## ФИЛИАЛ

<b>НФ</b>	<b>АДР_Ф</b>
-----------	--------------

## МЕНЕДЖЕР–ФИЛИАЛ

<b>НМ</b>	<b>НФ</b>
-----------	-----------

При этом осуществляется декомпозиция связи 1:1 на две связи 1:1 следующим образом:



Для связи типа 1:M существуют только два правила. Выбор одного из них зависит от класса принадлежности сущности на стороне M. Класс принадлежности сущности на стороне 1 не влияет на выбор.

#### Правило 4

Если связь типа 1:M и класс принадлежности сущности на стороне M является обязательным, то необходимо построить таблицу для каждой сущности. Первичный ключ сущности должен быть первичным ключом соответствующей таблицы. Первичный ключ сущности на стороне 1 добавляется как атрибут в таблицу для сущности на стороне M.

На ER-диаграмме связи 1:M, представленной на рис. 7, класс принадлежности сущности СЧЕТ является обязательным. Тогда согласно правилу 4 должны быть сгенерированы две таблицы следующей структуры:

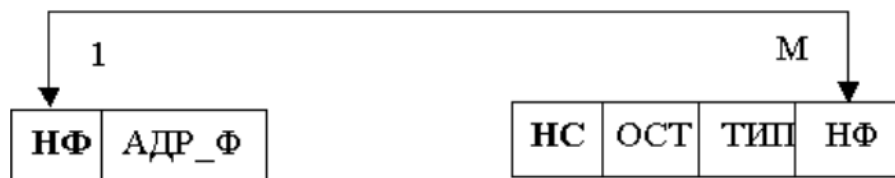
### ФИЛИАЛ

<b>НФ</b>	АДР_Ф
-----------	-------

### СЧЕТ– ФИЛИАЛ

<b>НС</b>	ОСТ	ТИП	НФ
-----------	-----	-----	----

Связь между указанными таблицами будет иметь вид:



Примечание. Если внешний ключ представляет связь 1:M, то должны быть разрешены его дублирующие значения.

### Правило 5

Если связь типа 1:M и класс принадлежности сущности на стороне M является необязательным, то необходимо построить три таблицы – по одной для каждой сущности и одну для связи. Первичный ключ сущности должен быть первичным ключом соответствующей таблицы. Таблица для связи среди своих атрибутов должна иметь ключи обеих сущностей.

Представим, что на ER-диаграмме связи 1:M, изображенной на рис. 7, класс принадлежности сущности СЧЕТ является необязательным. Тогда согласно правилу 5 должны быть сгенерированы три таблицы следующей структуры:

### ФИЛИАЛ

<b>НФ</b>	АДР_Ф
-----------	-------

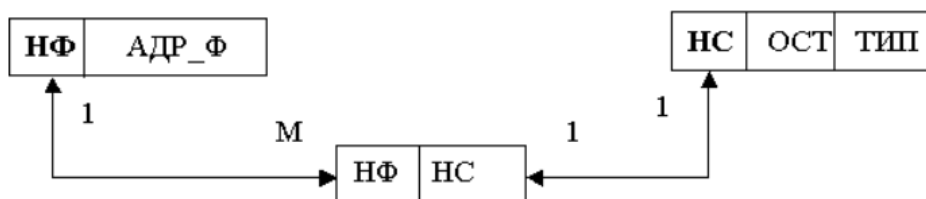
### СЧЕТ

<b>НС</b>	ОСТ	ТИП
-----------	-----	-----

### ФИЛИАЛ – СЧЕТ

<b>НФ</b>	<b>НС</b>
-----------	-----------

При этом осуществляется декомпозиция связи 1:M на две связи – 1:M и 1:1 – следующим образом



Для связи типа M:N класс принадлежности сущности не имеет значения.

#### Правило 6

Если связь типа M:N, то необходимо построить три таблицы – по одной для каждой сущности и одну для связи. Первичный ключ сущности должен быть первичным ключом соответствующей таблицы. Таблица для связи среди своих атрибутов должна иметь ключи обеих сущностей.

ER-диаграмма связи M:N имеется на рис. 7. Согласно правилу 6 на основе этой ER-диаграммы должны быть сгенерированы три таблицы следующей структуры:

#### КЛИЕНТ

<b>НК</b>	<b>ФИО_К</b>	<b>СОЦ_П</b>	<b>АДР_К</b>
-----------	--------------	--------------	--------------

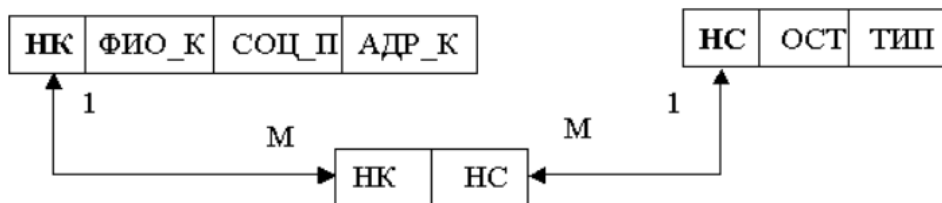
#### СЧЕТ

<b>НС</b>	<b>ОСТ</b>	<b>ТИП</b>
-----------	------------	------------

#### КЛИЕНТ– СЧЕТ

<b>НК</b>	<b>НС</b>
-----------	-----------

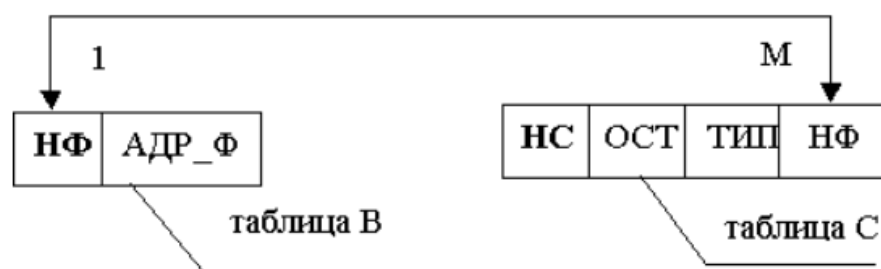
При этом осуществляется декомпозиция связи M:N на две связи 1:M следующим образом:



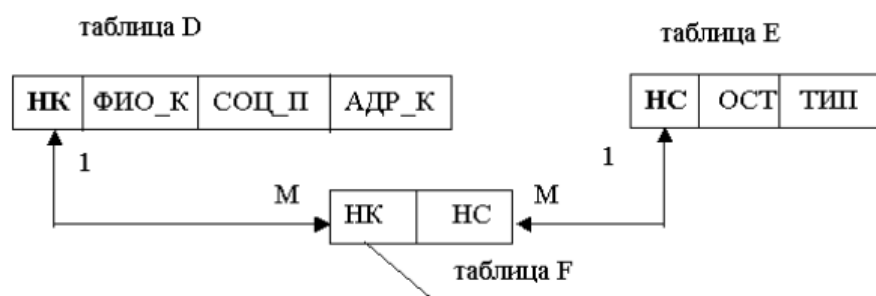
В таблице КЛИЕНТ–СЧЕТ клиенту, имеющему, например, три счета будут соответствовать три строки с одним и тем же номером клиента. А счет, у которого, например, два владельца, представляется двумя строками с различными номерами клиентов, владеющими этим счетом. К ER-модели предметной области БАНК, представленной на рис. 7, применимы правила 1, 4, 6. Связь МЕНЕДЖЕР – ФИЛИАЛ представляется (согласно правилу 1) одной таблицей А:

<b>НМ</b>	<b>СТАЖ</b>	<b>СПЕЦ</b>	<b>НФ</b>	<b>АДР_Ф</b>
-----------	-------------	-------------	-----------	--------------

Связь ФИЛИАЛ – СЧЕТ представляется (согласно правилу 4) связью:



Связь КЛИЕНТ – СЧЕТ представляется (согласно правилу 6) связью:



Анализ состава атрибутов полученных таблиц А, В, С, D, E, F показывает, что таблица В является составной частью таблицы А, таблица Е – составной частью таблицы С. Поэтому таблицы В, Е можно исключить из рассмотрения. Оставшиеся таблицы А, С, D, F можно связать посредством связи первичных и внешних ключей. В результате получим реляционную модель для ER-модели предметной области БАНК.

3. **Нормализация таблиц.** Для правильного выполнения нормализации проектировщик должен глубоко изучить семантику и особенности использования данных. На этом шаге он проверяет корректность структуры таблиц, созданных на предыдущем шаге, посредством применения к ним процедуры нормализации. Она заключается в приведении каждой из таблиц, по крайней мере, к 3НФ. В результате нормализации получается очень гибкий проект базы данных, позволяющий легко вносить в нее нужные расширения.

Нормализация таблиц - процесс, позволяющий минимизировать избыточность данных. Чтобы пояснить этот процесс, будем исходить из описания предметной области БАНК, представленного на рис. 7, и предположения, что на его основе была разработана база данных, состоящая из следующих двух таблиц:

**ФИЛИАЛ**

НФ	АДР_Ф	НМ	НС	ОСТ	ТИП
511	Ванеева, 6	7	1111 2222 3333	200 350 1000	Д Т Т
513	Солтыса, 3	9	5555 6666	800 14	Т Д

**КЛИЕНТ**

НК	ФИО_К	СОЦ_П	АДР_К	НС
23	Сокол С.С.	Служащий	Садовая, 1	1111 3333
34	Брас Б.Б.	Рабочий	Гая, 9	5555
45	Лань Л.Л.	Служащий	Лесная, 4	2222 6666 1111

1 нормальная форма (1НФ)

Таблица находится в 1НФ, если все ее поля содержат только простые неделимые значения.

Таблицы ФИЛИАЛ и КЛИЕНТ не удовлетворяют требованиям 1НФ. Для приведения их к 1НФ в них надо вставить новые записи следующим образом:



#### ФИЛИАЛ

НФ	АДР_Ф	НМ	НС	ОСТ	ТИП
511	Ванеева, 6	7	1111	200	Д
511	Ванеева, 6	7	2222	350	Т
511	Ванеева, 6	7	3333	1000	Т
513	Солтыса, 3	9	5555	800	Т
513	Солтыса, 3	9	6666	14	Д

#### КЛИЕНТ

НК	ФИО_К	СОЦ_П	АДР_К	НС
23	Сокол С.С.	Служащий	Садовая, 1	1111
23	Сокол С.С.	Служащий	Садовая, 1	3333
34	Брас Б.Б.	Рабочий	Гая, 9	5555
45	Лань Л.Л.	Служащий	Лесная, 4	2222
45	Лань Л.Л.	Служащий	Лесная, 4	6666
45	Лань Л.Л.	Служащий	Лесная, 4	1111

Но полученные таблицы неэффективны, так как содержат много избыточной информации. Необходимо их привести к 2НФ.

#### 2 нормальная форма (2НФ)

Таблица находится в 2НФ, если она удовлетворяет требованиям 1НФ и неключевые поля функционально полно зависят от первичного ключа.

Функциональная зависимость – это понятие, отображающее определенную семантическую связь между полями таблицы. Неключевое поле А функционально полно зависит от первичного ключа, если:

- 3.1 оно функционально зависит от первичного ключа, т.е. каждой комбинации значений полей первичного ключа соответствует одно и только одно значение поля А;
- 3.2 не существует функциональной зависимости А ни от какого подмножества полей первичного ключа (в противном случае А находится в частичной функциональной зависимости от первичного ключа).

В таблице КЛИЕНТ неключевые поля ФИО\_К, СОЦ\_П, АДР\_К функционально зависят от ключа (НК, НС). Кроме того, они функционально зависят от подмножества ключа – НК.

Следовательно, неключевые поля ФИО\_К, СОЦ\_П, АДР\_К находятся в частичной функциональной зависимости от первичного ключа (НК, НС) и нарушаются требования 2НФ. Эти поля надо из таблицы КЛИЕНТ удалить. Полученную в результате этого таблицу назовем КЛИЕНТ–СЧЕТ, которая имеет вид:

КЛИЕНТ–СЧЕТ

НК	НС
23	1111
23	3333
34	5555
45	2222
45	6666
45	1111

Эта таблица удовлетворяет требованиям 2НФ.

Удаленные неключевые поля помещаются в новую таблицу совместно с подмножеством НК, от которого они зависят. И это подмножество будет первичным ключом новой таблицы КЛИЕНТ вида:

КЛИЕНТ

НК	ФИО_К	СОЦ_П	АДР_К
23	Сокол С.С.	Служащий	Садовая, 1
34	Брас Б.Б.	Рабочий	Гая, 9
45	Лань Л.Л.	Служащий	Лесная, 4

Новая таблица КЛИЕНТ также удовлетворяет требованиям 2НФ. Ее неключевые поля функционально полно зависят от первичного ключа.

Полученные таблицы не содержат избыточной информации, и нет основания приводить их к 3НФ. Таблица ФИЛИАЛ удовлетворяет требованиям 2НФ, так как ее неключевые поля НФ, АДР\_Ф, НМ, ОСТ, ТИП функционально полно зависят от первичного ключа. Но в таблице ФИЛИАЛ повторяется информация о филиале для всех счетов, обрабатываемых им. Поэтому ее надо привести к 3НФ.

3 нормальная форма (3НФ)

Таблица находится в 3НФ, если она удовлетворяет требованиям 2НФ и не содержит транзитивных зависимостей.

Транзитивной зависимостью называется функциональная зависимость между неключевыми полями. В таблице ФИЛИАЛ она наблюдается. Следовательно, нарушаются требования 3НФ. Из таблицы ФИЛИАЛ надо удалить поля, участвующие в этой транзитивной зависимости, – АДР\_Ф, НМ. Получится таблица, характеризующая счет, вида:

**СЧЕТ**

НС	ОСТ	ТИП	НФ
1111	200	Д	511
2222	350	Т	511
3333	1000	Т	511
5555	800	Т	513
6666	14	Д	513

Затем создается новая таблица, в которую помещаются удаленные поля и поле, от которого они зависят. Она имеет вид:

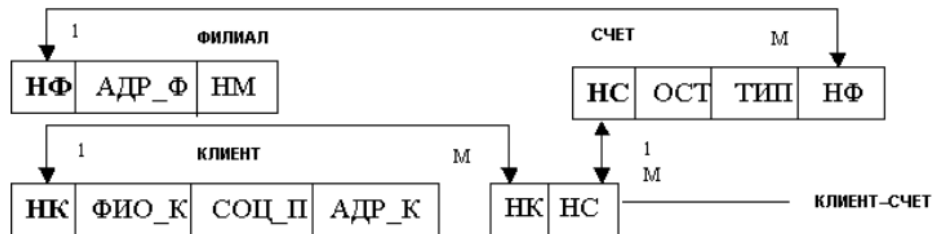
**ФИЛИАЛ**

НФ	АДР_Ф	НМ
511	Ванеева, 6	7
513	Солтыса, 3	9

Полученные таблицы приведены к 3НФ. В них каждая запись есть отдельное независимое утверждение. Повторяются только значения внешнего ключа НФ в таблице СЧЕТ, что неизбежно, так как одним филиалом могут обрабатываться несколько счетов.

Как видим, нормализация приводит к фрагментации исходных таблиц. В нашем примере таблица КЛИЕНТ разбивается на таблицы 1, 2, а таблица ФИЛИАЛ – на таблицы 3, 4. Осуще-

связав связь этих таблиц посредством связи первичных и внешних ключей, получим реляционную модель данных предметной области БАНК, в которой минимизирована избыточность данных:



4. **Проверка логической модели данных на предмет возможности выполнения всех транзакций, предусмотренных пользователями.** Транзакция – это набор действий, выполняемых отдельным пользователем или прикладной программой с целью изменения содержимого базы данных. Так, примером транзакции в проекте БАНК может быть передача права распоряжаться счетами некоторого клиента другому клиенту. В этом случае в базу данных потребуется внести сразу несколько изменений. Если во время выполнения транзакции произойдет сбой в работе компьютера, то база данных окажется в противоречивом состоянии, так как некоторые изменения уже будут внесены, а остальные еще нет. Поэтому все частичные изменения должны быть отменены для возвращения базы данных в прежнее непротиворечивое состояние.

Перечень транзакций определяется действиями пользователей в предметной области. Используя ER-модель, словарь данных и установленные связи между первичными и внешними ключами, производится попытка выполнить все необходимые операции доступа к данным вручную. Если какую-либо операцию выполнить вручную не удастся, то составленная логическая модель данных является неадекватной и содержит ошибки, которые надо устранить. Возможно, они связаны с пропуском в модели сущности, связи или атрибута.

5. **Определение требований поддержки целостности данных и их документирование.** Эти требования представляют собой ограничения, которые вводятся с целью предотвратить помещение в базу данных противоречивых данных. На этом шаге вопросы целостности данных освещаются безотносительно к конкретным аспектам ее реализации. Должны быть рассмотрены следующие типы ограничений:

- обязательные данные. Выясняется, есть ли атрибуты, которые не могут иметь Null-значений;
- ограничения для значений атрибутов. Определяются допустимые значения для атрибутов;
- целостность сущностей. Она достигается, если первичный ключ сущности не содержит Null-значений;
- ссылочная целостность. Она понимается так, что значение внешнего ключа должно обязательно присутствовать в первичном ключе одной из строк таблицы для родительской сущности;

- ограничения, накладываемые бизнес-правилами. Например, в случае с проектом БАНК может быть принято правило, запрещающее клиенту распоряжаться, скажем, более чем тремя счетами.

Сведения обо всех установленных ограничениях целостности данных помещаются в словарь данных.

6. **Создание окончательного варианта логической модели данных и обсуждение его с пользователями.** На этом шаге подготавливается окончательный вариант ER-модели, представляющей логическую модель данных. Сама модель и обновленная документация, включая словарь данных и реляционную схему связи таблиц, представляется для просмотра и анализа пользователям, которые должны убедиться, что она точно отражает предметную область.

### 9.3.6 Физическое проектирование

Цель этапа физического проектирования – описание конкретной реализации базы данных, размещаемой во внешней памяти компьютера. Это описание структуры хранения данных и эффективных методов доступа к данным базы. При логическом проектировании отвечают на вопрос – что надо сделать, а при физическом – выбирается способ, как это сделать. Процедуры физического проектирования следующие:

1. **Проектирование таблиц базы данных средствами выбранной СУБД.** Осуществляется выбор реляционной СУБД, которая будет использоваться для создания базы данных, размещаемой на машинных носителях. Глубоко изучаются ее функциональные возможности по проектированию таблиц. Затем выполняется проектирование таблиц и схемы их связи в среде СУБД. Подготовленный проект базы данных описывается в сопроводительной документации.
2. **Реализация бизнес-правил в среде выбранной СУБД.** Обновление информации в таблицах может быть ограничено бизнес-правилами. Способ их реализации зависит от выбранной СУБД. Одни системы для реализации требований предметной области предлагают больше возможностей, другие – меньше. В некоторых системах вообще отсутствует поддержка реализации бизнес-правил. В таком случае разрабатываются приложения для реализации их ограничений. Все решения, принятые в связи с реализацией бизнес-правил предметной области, подробно описываются в сопроводительной документации.
3. **Проектирование физической организации базы данных.** На этом шаге выбирается наилучшая файловая организация для таблиц. Выявляются транзакции, которые будут выполняться в проектируемой базе данных, и выделяются наиболее важные из них. Анализируется пропускная способность транзакций – количество транзакций, которые могут быть обработаны за заданный интервал времени, и время ответа – промежуток времени, необходимый для выполнения одной транзакции. Стремятся к повышению пропускной способности транзакций и уменьшению времени ответа. На основании указанных показателей принимаются решения об оптимизации производительности базы данных путем определения индексов в таблицах, ускоряющих выборку данных из базы, или снижения требований к уровню нормализации таблиц. Проводится оценка дискового объема памяти, необходимого для размещения создаваемой базы данных. Стремятся к его минимизации. Принятые решения по изложенным вопросам документируются.

4. **Разработка стратегии защиты базы данных.** База данных представляет собой ценный корпоративный ресурс, и организации ее защиты уделяется большое внимание. Для этого проектировщики должны иметь полное и ясное представление обо всех средствах защиты, предоставляемых выбранной СУБД.
5. **Организация мониторинга функционирования базы данных и ее настройка.** После создания физического проекта базы данных организуется непрерывное слежение за ее функционированием. Полученные сведения об уровне производительности базы данных используются для ее настройки. Для этого привлекаются и средства выбранной СУБД.

Решения о внесении любых изменений в функционирующую базу данных должны быть обдуманными и всесторонне взвешенными.

## 9.4 Формальные верификации и спецификации

Оценивание качества программного обеспечения информационных систем неразрывно связано с процессом верификации, т. е. с подтверждением того, что функциональные возможности ПО соответствуют их описаниям в программной документации (т.е. их спецификации). Функциональные возможности, которые не имеют описания в документации или не соответствуют описанию, называются недекларированными возможностями. Они могут являться как следствием ошибок разработчика, так и результатом выполнения умышленно внедрённого в программу кода. Как случайные, так и преднамеренные НДВ (последние называются также программными закладками) представляют угрозу информационной безопасности программных систем. Цель верификации программ – выявление и регистрация НДВ для последующего их устранения.

Любое программное средство обладает определённой корректностью. Понятие корректность является более узким, чем понятие качество, так как последнее включает в себя такие характеристики, как надёжность, мобильность, понятность, сопровождаемость программной системы. Корректность характеризует функциональные возможности программы, т. е. одну из составляющих качества. Корректность программы наиболее полно определяется степенью её соответствия программной спецификации.

В настоящее время существует множество методов и средств автоматизированной верификации ПО, часто применяемых совместно, взаимно дополняющих друг друга. Но не менее важным, чем ПО, компонентом ИС является база данных. Она также оказывает влияние на качество ИС и нуждается в верификации. Для проведения полноценной верификации требуется:

- правильное понимание сущности БД;
- система количественных и качественных показателей корректности БД;
- наличие автоматизированных систем верификации БД.

На современном этапе БД должны рассматриваться не только как хранилища данных, но и как полноценные программные компоненты. Обоснованием данного положения служит практика использования промышленных СУБД и ИС, основанная в значительной степени на использовании клиент-серверной архитектуры и технологии активного сервера. Суть последней заключается в том, что функции ИС, выполняющие обработку данных в БД, реализуются не в клиентских приложениях, а на стороне сервера СУБД в виде хранимых подпрограмм БД. Слово «хранимый» указывает

на то, что коды этих подпрограмм располагаются вместе с данными и являются, таким образом, объектами БД.

Известно три типа хранимых подпрограмм: функции, процедуры и триггеры.

Функции и процедуры запускаются на выполнение путём явного вызова. Клиентскому приложению, чтобы вызвать процедуру, необходимо предварительно соединиться с БД, где расположен ее откомпилированный код. Обращение к процедуре производится по имени с передачей входных данных и, возможно, с заданием выходных параметров. Функция отличается от процедуры тем, что она всегда возвращает атомарное значение определённого типа и вызывается путем использования в арифметических и логических выражениях на месте операнда.

Триггер – это специальный тип хранимых подпрограмм. Он выполняется автоматически в ответ на вставку, обновление или удаление записей в таблице и служит для поддержания корректности и согласованности (целостности) данных. Реализация хранимых подпрограмм возможна как на языке баз данных, так и на языках программирования высокого уровня C, C++, Pascal, Java.

Из сказанного следует, что БД, поддерживаемые промышленными СУБД имеют двойственную природу. Оставаясь хранилищами данных, они одновременно играют роль программного обеспечения в ИС или, точнее, становятся полноценными программными компонентами, напоминающими динамически подключаемые библиотеки операционной системы Windows или СОМ-объекты. Как и любая другая часть ИС, БД нуждаются в верификации и тестировании.

Учитывая то, что верификация есть подтверждение корректности, необходимо заметить, что корректность БД должна оцениваться при помощи системы математических показателей. К числу наиболее часто встречающихся сегодня на практике функциональных показателей корректности БД относятся следующие:

- **полнота накопленных описаний объектов** – относительное число объектов и документов, имеющих в БД, к общему числу объектов в аналогичной БД;
- **достоверность** – степень соответствия записей БД реальным объектам в данный момент времени;
- **идентичность данных** – относительное число описаний объектов, не содержащих ошибки, к общему числу документов об объектах в БД;
- **актуальность данных** – относительное число устаревших данных к общему числу накопленных и обрабатываемых записей.

Помимо функциональных показателей, существуют конструктивные показатели корректности, отличающиеся большей универсальностью, независимостью от сферы применения базы данных:

- **объем БД** – число описаний объектов или документов в БД, доступных для хранения и обработки;
- **оперативность** – степень соответствия динамики изменения данных в процессе сбора и обработки состояниям реальных объектов, или величина запаздывания между появлением (изменением) характеристик реального объекта и его отражением в БД;
- **периодичность** – промежуток времени между поставками двух последовательных, достаточно различающихся информацией версий БД;

- **глубина ретроспективы** – интервал времени от даты выпуска (записи в БД) самого раннего документа до настоящего времени;
- **динамичность** – относительное число изменяемых описаний объектов к общему числу записей в БД за некоторый интервал времени, определяемый периодичностью издания версий БД.

Оценивание корректности БД предполагает анализ ее содержимого, логической структуры и программной составляющей (хранимых подпрограмм). В связи с этим необходимо различать три вида корректности БД: корректность содержимого, корректность схемы данных и программная корректность. Рассмотрим каждый из перечисленных видов по отдельности.

**Корректность содержимого.** Любая запись в БД должна адекватно отражать характеристики реального существующего объекта, экземпляра сущности предметной области; если же в записи фиксируется информация о взаимодействии объектов, то речь должна идти о взаимодействии, имеющем место в реальной действительности.

Очевидно, что корректность содержимого определяется функциональными и конструктивными показателями, рассмотренными выше.

**Корректность схемы данных.** Традиционно под реляционной схемой понимается набор взаимосвязанных схем отношений или, с точки зрения обычного пользователя, весь набор таблиц БД. Можно выделить следующие подвиды корректности схемы данных:

#### 1. Точность отображения концептуальной схемы (ER-схемы) на реляционную.

Концептуальная модель реляционной БД обычно представляется в виде диаграмм сущность–связь, или ER-диаграмм, на которых показываются объекты предметной области и связи (способы взаимодействия) между ними. При концептуальном проектировании не оперируют понятиями «таблица», «внешний ключ» и т. п. Но ER-диаграммы легко преобразуются в схему реляционной БД по набору типовых правил. В итоге сущностям, представленным на ER-схеме, соответствуют таблицы реляционной БД, а связям – вспомогательные таблицы и внешние ключи. Типовые правила отображения дают возможность «обратного проектирования» – получения ER-схемы по имеющейся реляционной схеме БД. Однако не всегда «обратное проектирование» даёт ER-схему, эквивалентную исходной концептуальной модели. Причиной этого в ряде случаев является неточность прямого преобразования, в результате чего схема БД получается некорректной по отношению к исходной ER-модели.

Точность отображения, очевидно, может быть определена как соответствие ER-схемы, полученной в результате «обратного проектирования», исходной концептуальной схеме. Точность отображения характеризуется множеством показателей, учитывающих детализацию сравнения на уровне атрибутов, сущностей, связей и участков ER-диаграмм, образованных двумя отдельно взятыми сущностями и одной ассоциацией между ними.

В каждом случае необходимо рассчитывать относительное число правильно отображенных на реляционную схему сущностей, атрибутов, связей и участков, к общему числу соответствующих элементов, определенных на этапе концептуального проектирования. С другой стороны, в процессе создания реляционной схемы могут появиться недекларированные атрибуты, сущности и связи. Процесс верификации БД должен включать в себя оценивание их процентного



содержания в общем числе отраженных на реляционной схеме сущностей, атрибутов и связей соответственно. Чем ниже процентное содержание недекларированных элементов схемы данных, тем корректнее БД по отношению к концептуальной модели.

## **2. Нормализованность таблиц.**

Основная цель проектирования БД – группирование атрибутов по таблицам так, чтобы минимизировать избыточность данных и по возможности сократить объём памяти, необходимый для физического хранения таблиц. Теория нормальных форм и нормализации описывает один из формальных методов проектирования БД, в котором идентификация таблиц основана на выявлении первичных ключей и функциональных зависимостей между атрибутами.

Высшей нормальной формой на практике оказывается, как правило, нормальная форма Бойса–Кодда. Согласно её требованиям, все неключевые атрибуты таблицы должны полностью функционально зависеть от потенциального ключа, а функциональных зависимостей между различными неключевыми атрибутами быть не должно. Нарушение этих требований приводит к избыточности данных и, как следствие, к аномалиям вставки, обновления и удаления записей.

Современные методы проектирования (в том числе упомянутый ранее метод ER-моделирования) позволяют автоматически приводить таблицы БД к нормальной форме Бойса–Кодда. Однако ошибки могут возникать, особенно если разработчиками принимается нешаблонное решение о частичной денормализации таблиц.

Проще всего оценивать нормализованность БД при помощи относительного числа полностью нормализованных таблиц к общему числу таблиц. Более сложной задачей является оценивание степени допустимости денормализации для данного проекта, если таковая имеет место.

## **3. Логическая целостность.**

Важной составляющей корректности схемы данных является логическая целостность. С каждой предметной областью связаны определённые требования целостности, которые тем или иным образом ограничивают диапазоны возможных значений атрибутов сущностей и связей, говорят о допустимости либо недопустимости комбинаций некоторых значений. Реализация требований целостности в БД позволяет избавиться от появления отрицательных возрастов и масс, от повторения одного и того же ИНН у различных лиц, от некорректной последовательности дат начала и завершения работы (в случае, когда они в результате ошибки пользователя меняются местами) – словом, избежать появления логически противоречивой, несогласованной, «невозможной» с позиции здравого смысла информации.

Простые требования целостности реализуются при помощи специальных объектов БД, называемых ограничениями. Большинство реляционных СУБД сегодня поддерживают такие ограничения целостности, как первичный ключ, внешний ключ, уникальность значений, запрет неопределённых значений и ограничение на основе логического условия. Более сложные требования целостности реализуются процедурно с помощью специальных подпрограмм – триггеров. Следует заметить, что целостность в данном случае пересекается с программной корректностью, которая будет рассматриваться далее. И в первом, и во втором случае речь идёт об автоматическом поддержании целостности. Во время выполнения операций вставки,

удаления и обновления неверные данные либо не принимаются совсем, либо автоматически корректируются.

Целесообразно оценивать логическую целостность БД при помощи следующих показателей.

- **Полнота реализации требований целостности** – отношение реализованных в БД ограничений и триггеров к общему числу заявленных требований. Ограничения, которые не были заявлены в документации, не рассматриваются.
- **Относительное число не заявленных в документации ограничений целостности к общему числу реализованных.** Если недекларированных ограничений нет, показатель принимает нулевое значение, что говорит о корректности схемы данных.
- **Согласованность ограничений с содержимым таблиц.** Возможны ситуации, когда дополнительное ограничение целостности или новый триггер добавляются в уже заполненную БД. При этом нельзя допустить, чтобы новое ограничение вошло в противоречие с уже добавленными в таблицы записями. Для обычных ограничений целостности эта проблема решена на уровне СУБД. Система запрещает вводить ограничение, если в БД уже имеются строки таблиц, которые ему не удовлетворяют. Но СУБД не в состоянии выполнить подобную проверку для триггера. Поэтому возможны противоречия: с одной стороны, имеется сложное ограничение целостности, реализуемое триггером; с другой стороны, записи, появившиеся в БД до создания триггера, могут заведомо не удовлетворять этому ограничению.

Показатель согласованности ограничений и содержимого таблиц рассчитывается как отношение записей, удовлетворяющих всем ограничениям, к общему числу записей. Расчет этого показателя неразрывно связан с анализом программного кода триггеров, цель которого – выяснить декларативный смысл каждого триггера. Задача эта сама по себе нетривиальна и требует отдельного рассмотрения.

- **Непротиворечивость ограничений.** В результате ошибок проектирования в БД могут возникать конфликты между ограничениями и триггерами. Когда разные триггеры и ограничения предъявляют к данным противоречивые требования, вплоть до взаимоисключающих, таблицы БД могут оказаться недоступными для вставки и обновления строк.

Свойство непротиворечивости ограничений затруднительно оценить количественно. Вероятно, речь должна идти о качественном показателе или комплексе количественных и качественных показателей, позволяющих оценить степень изолированности самих ограничений друг от друга, степень доступности данных, с которыми связано множество ограничений и триггеров, а также долю противоречивых ограничений во всей БД.

- **Сложность реализации требования целостности.** Даже простые ограничения могут быть реализованы с помощью триггеров. Теоретически это допустимо, но на практике подобные решения снижают эффективность системы. Кроме того, очевидно, что они затрудняют последующую верификацию БД, увеличивают время анализа, так как приходится восстанавливать декларативный смысл каждого триггера. Декларативный смысл обычного ограничения целостности всегда ясен из его описания.

Сложность реализации требования целостности – качественный показатель, оцениваемый для каждого триггера. Если данное требование может быть полностью реализовано

при помощи стандартных ограничений, сложность является очень высокой. В противном случае вычисление показателя производится на основе семантического анализа команд, выполняемых в теле триггера. Возможные значения показателя сложности реализации: «очень низкая», «низкая», «средняя», «высокая», «очень высокая».

#### 4. Программная корректность баз данных.

Корректность программных процедур существенно зависит от их топологической и информационной сложности: чем выше сложность, тем больше вероятность появления неумышленных НДВ, с одной стороны, и тем сильнее усложняется обнаружение любых НДВ, с другой стороны.

К настоящему времени предложено множество метрик оценивания сложности программ. Оценивание сложности хранимых подпрограмм БД может производиться с использованием метрик размера программ и метрик сложности потока управления.

Исходя из сказанного, можно определить следующие характеристики программной сложности БД:

- **Суммарная сложность подпрограмм БД.** Вычисляется как алгебраическая сумма сложностей (весов) всех подпрограмм. С тем, какой именно показатель (из перечисленных выше) будет характеризовать сложность отдельно взятой подпрограммы, необходимо определиться заранее, до выполнения вычислений.
- **Группа показателей, отражающая наличие сцепления между подпрограммами.** Сцепление подпрограмм имеет место в том случае, если они используют общие атрибуты таблиц. Малое сцепление в программном классе или компоненте желательно, поскольку оно увеличивает инкапсуляцию и снижает вероятность возникновения ошибок в поведении компонента. Наиболее простым показателем сцепления является разность между числом пар несцепленных и числом пар сцепленных подпрограмм. Отрицательный показатель сцепления всегда приравнивается к нулю.