Основы построения защищенных баз данных

Ваша команда по спасению компьютерной безопасности

11 марта 2020 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

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**[1]– 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)**[1] – 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 приходиться говорить о вопросах безопасности, все превращается в классическую задачу о двух стульях: как надо и как в законе написано. (Ну или пафосно перефразируя) Вопросы информационной безопасности баз данных целесообразно рассматривать с двух взаимодополняющих позиций **Al2015**[**Lihonosov2011**][2]:

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

[1] Нагло скопипизженно с вечно загнивающей
[2] Мне стыдно указывать ресурс, где я взял этот кусок, так что пусть будет pornhub

Попытка защищать все и сразу обречена на провал, так что довольно логичным кажется сосредоточится на обеспечении безопасности четырех уровней информационной системы:

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[3].

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

- **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.
- **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

[3] А эти определения я взял с прошлого года

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

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.

Сформулируем перечень внешних и внутренних угроз информационной безопасности баз данных.

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

Угрозы, специфичные для систем управления базами данных:

1. Угрозы конфиденциальности информации:
    - инъекция SQL. Во многих приложениях используется динамический SQL – формирование SQL-предложений кодом программы путем конкатенации строк и значений предметов. 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
    - логический вывод на основе функциональных зависимостей. Пример функциональной зависимости для схемы отношения (фамилия, имя, отчество, должность, зарплата): если должность = менеджер, то зарплата = 1200. В реальных БД при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение
    - логический вывод на основе ограничений целостности. Для кортежей отношений в реляционной модели данных можно задать ограничения целостности – логические условия, которым должны удовлетворять атрибуты кортежей. Причем ограничение целостности может быть задано в виде предиката на всем множестве атрибутов кортежа. В случае попытки изменения данных в таблицу, СУБД автоматически вычисляет значение этого предиката, и в зависимости от его истинности операция разрешается или отвергается. Выполняя многократные изменения данных и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него отсутствует непосредственный доступ. Также к этому виду угроз конфиденциальности относится анализ значений первичных/внешних ключей
    - использование оператора UPDATE для получения конфиденциальной информации. В некоторых стандартах SQL пользователь, не обладая привилегией на выполнение оператора SELECT, мог выполнить оператор UPDATE со сколь угодно сложным логическим

условием. Так как после выполнения оператора UPDATE сообщается, сколько строк он обработал, фактически пользователь мог узнать, существуют ли данные, удовлетворяющие этому условию

2. Угрозы целостности информации:

   - модификация данных в реляционных СУБД возможна с помощью SQL-операторов UPDATE, INSERT и DELETE. Потенциальная опасность возникает из-за того, что пользователь, обладающий соответствующими привилегиями, может модифицировать все записи в таблице. Ограничить множество записей, доступных для модификации, можно с помощью создания представлений с оператором CHECK, но этот (равно как и любой другой) требует предварительного осмысления существа задачи и соответствующего проектирования схемы

3. Угрозы доступности:

   - использование свойств первичных и внешних ключей. В первую очередь сюда относится свойство уникальности первичных ключей и наличие ссылочной целосности. В том случае, если используются натуральные, а не генерируемые системой значения первичных ключей, можно создать такую ситуацию, когда в таблицу невозможно будет вставить новые записи, так как там уже будут записи с такими же значениями первичных ключей. Если в базе данных поддерживается ссылочная целостность, можно организовать невозможность удаления родительских записей, умышленно создав подчиненные записи. Важной особенностью реализации ссылочной целостности является вопрос об индексировании внешнего ключа. В том случае, если внешний ключ не проиндексирован, то при обновлении связанных записей, например, в СУБД Oracle возможна организация взаимной блокировки (dead-lock), что приведет к сбою транзакции
   - блокировка записей при изменении. Заблокировав записи или всю таблицу, злоумышленник может на значительное время сделать ее недоступной для обновления
   - загрузка системы бессмысленной работой. Простейший пример – выполнение запроса, содержащего декартово произведение двух больших отношений. При выдаче злоумышленником запроса вида SELECT * FROM Tab1, Tab1 ORDER BY 1, где мощность отношения (количества строк в таблицу Tab1) $N = 10000$, мощность результирующего отношения будет $N \times N = 10^8$. Вычисления соединения и сортировка результирующего отношения потребуют значительных ресурсов системы и отрицательно скажутся на производительности операций других пользователей

1.0.3 Требования безопасности БД

[4] На основании угроз можно выделить следующий список требований к безопасности БД:

- 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

[4] Прошлый год

- 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

1.0.4 Защита от несанкционированного доступа

[5] К основным средствам защиты информации относят следующие:

- 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 устанавлюваются конечным 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, 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

[5] Прошлый год

управления доступа, организация доступа пользователей по предъявлению сертификата, выборочное шифрование для сегментов базы данных.

1.0.5 Защита от вывода

[6]

Логический вывод на основе функциональных зависимостей. Пусть дана схема отношения: $R(A_1, \ldots, A_n)$. Пусть $U = (A_1, \ldots, A_n)$, X, Y – подмножества из U. Говорят, что X функционально определяет Y, если в любом отношении r со схемой $R(A_1, \ldots, A_n)$ не могут содержаться два кортежа с одинаковыми значениями атрибутов из X, с различными из Y. В этом случае имеет место функциональная зависимость, обозначаемая . Пример функциональной зависимости для схемы отношения (фамилия, имя, отчество, должность, зарплата): если должность = менеджер, то зарплата = 1200. В реальных базах данных при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.

Логический вывод на основе ограничений целостности. Для кортежей отношений в реляционной модели данных (РМД) можно задать ограничения целостности — логические условия, которым должны удовлетворять атрибуты кортежей. Причем ограничение целостности может быть задано в виде предиката на всем множестве атрибутов кортежа. В случае попытки изменения данных в таблице, СУБД автоматически вычисляет значение этого предиката, и в зависимости от его истинности операция разрешается или отвергается. Выполняя многократные изменения данных и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него отсутствует непосредственный доступ. Также к этому виду угроз конфиденциальности относится анализ значений первичных/внешних ключей.

1.0.6 Целостность БД

Целостность базы данных – соответствие имеющейся в базе данных информации её внутренней логике, структуре и всем явно заданным правилам. Каждое правило, налагающее некоторое ограничение на возможное состояние базы данных, называется ограничением целостности.

Очевидно, что ограничения должны быть формально объявлены для СУБД, после чего СУБД должна предписывать их выполнение. Объявление ограничений сводится просто к использованию соответствующих средств языка базы данных, а соблюдение ограничений осуществляется с помощью контроля со стороны СУБД над операциями обновления, которые могут нарушить эти ограничения, и запрещения тех операций, которые их действительно нарушают. При первоначальном объявлении ограничения система должна проверить, удовлетворяет ли ему в настоящий момент база данных. Если это условие не соблюдается, ограничение должно быть отвергнуто; в противном случае оно принимается (то есть записывается в каталог системы) и начиная с этого момента соблюдается.

В теории реляционных баз данных принято выделять четыре типа ограничений целостности:

- Ограничением базы данных называется ограничение на значения, которые разрешено принимать указанной базе данных.

[6] Взял hrefhttp://www.e-biblio.ru/book/bib/01_informatika/b_baz_dan/sg.htmlздесь

- Ограничением переменной отношения называется ограничение на значения, которые разрешено принимать указанной переменной отношения.
- Ограничением атрибута называется ограничение на значения, которые разрешено принимать указанному атрибуту.
- Ограничение типа представляет собой не что иное, как определение множества значений, из которых состоит данный тип.[7]

1.0.7 Аудит

Важнейшей составляющей процесса обеспечения безопасности ИС является проведение квалифицированного аудита. Несмотря на то, что подготовка и проведение профессионального аудита безопасности ИС требует существенных финансовых и кадровых затрат, высшее руководство многих организаций считает подобные затраты оправданными.

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 решаемыми задачами организации уровню.

Ядром построения ИС предприятия является СУБД промышленного уровня, Полноценная система обеспечения безопаности 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 системе в словаре данных или специальном файле – журнале аудита. Информация о настройках системы аудита хранятся 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

1. Физическая защита

[7] Подробнее про ограничения: https://studfiles.net/preview/6354061/page:55/ (Блядский роскомнадзор будет ругаться, но вас это пугать не должно)

(a) Прежде всего, необходима физическая защита информации: чтобы сервер с данными не был похищен. Для этого сервера располагают в охраняемом дата-центре с видеонаблюдением и ограниченным доступом лиц в эти помещения

(b) Второй уровень физической защиты — обеспечение сохранности самих данных, содержащихся на этих серверах. Этот вопрос решается применением политики резервного копирования информации

2. Защита ОС: Различные средства от НСД и прочее.

3. Защита на уровне передачи данных: Передача данных тоже нуждается в защите, поскольку существует вероятность перехвата информации в момент ее транзита. Шифрование траффика позволяет защитить данные системы от перехвата снифферами и т.п.

4. Авторизация в системе: Различные виды идентификации и аутентификации.

5. Система прав и объектов: Различные модели разграничения доступа.

1.0.9 Типы контроля безопасности: потоковый, контроль вывода, контроль доступа[None]

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 категорированной 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 должен 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 эффективность 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

Политика безопаности – это набор законов, правил, процедур и норм поведения, определяющих, 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[None]

2.1.4 Интерпретация TCSEC для надежных СУБД (TDI)[None]

2.1.5 Оценка надежности СУБД как компоненты вычислительной системы[None]

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[None]

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

https://web.archive.org/web/20160303230445/http://ftp.fas.org/irp/nsa/rainbow/tg021.htm

2.1.9 Критерии безопасности ГТК

https://fstec.ru/component/attachments/download/293

2.2 Модели безопасности в СУБД

Дискреционная (избирательная) и мандатная (полномочная) модели безопасности

Классификация моделей

Аспекты исследования моделей безопасности

Особенности применения моделей безопасности в СУБД

Дискреционные модели: HRU, Take-Grant, Action-Entity, Wood

Мандатные модели: Bell-LaPadula, Biba, Dion, Sea View, Jajodia&Sandhu, Smith&Winslett, решеточная

БД с многоуровневой секретностью (MLS)

Многозначность

3 Полезные ссылки

1. Какие-то лекции – есть шанс, что они морально устарели еще до нашего поступления.
2. Вроде норм книга – осторожней, без адблока заходить больно для глаз.