САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

Безопасность систем баз данных

Лекция 1
Введение

Агафонов Антон Александрович
к.т.н., доцент кафедры ГИиИБ

Самара

План курса

- Аутентификация и доступ к данным
- Резервное копирование данных
- Репликация
- Балансировка нагрузки
- Аудит и мониторинг
- Шифрование
- Целостность данных
- SQL-инъекции

План лекции

- Понятие защищенной базы данных
- Источники угроз информационной безопасности
- Основные принципы обеспечения безопасности
- Особенности систем БД как объекта защиты
- Угрозы безопасности БД
- Методы защиты

Понятие защищенной БД

Защищенная база данных – это БД, которая обеспечивает конфиденциальность, доступность и целостность данных пользователя.

- **Конфиденциальность** отвечает за обеспечение доступа к данным только санкционированным пользователями.
- **Целостность** исключает несанкционированное изменение структуры и содержания данных.
- **Доступность** позволяет обеспечить доступ к данным санкционированным пользователями по их первому требованию.

Конфиденциальность

Конфиденциальность информации — необходимость предотвращения разглашения, утечки какой-либо информации.

Конфиденциальность информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомлённости (англ. need-to-know). Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей.

Одной из важнейших мер обеспечения конфиденциальности является классификация информации, которая позволяет отнести её к строго конфиденциальной, или предназначенной для публичного, либо внутреннего пользования.

Шифрование информации — характерный пример одного из средств обеспечения конфиденциальности.

Целостность

Целостность информации — термин, означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки.

Помимо преднамеренных действий, во многих случаях неавторизованные изменения важной информации возникают в результате технических сбоев или человеческих ошибок.

Для защиты целостности информации необходимо применение разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Типичным примером таких мер является ограничение круга лиц с правами на изменения лишь теми, кому такой доступ необходим для выполнения служебных обязанностей. Кроме того, любые изменения в ходе жизненного цикла информационных системы должны быть согласованы, протестированы на предмет обеспечения информационной целостности и внесены в систему только корректно сформированными транзакциями.

Доступность

Доступность информации — состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации.

Основными факторами, влияющими на доступность информационных систем, являются DoS-атаки (Denial of Service — «отказ в обслуживании»), атаки программ-вымогателей, саботаж. Кроме того, источником угроз доступности являются непреднамеренные человеческие ошибки.

Во всех случаях конечный пользователь теряет доступ к информации, необходимой для его деятельности, возникает вынужденный простой. Критичность системы для пользователя и её важность для выживания организации в целом определяют степень воздействия времени простоя. Недостаточные меры безопасности увеличивают риск поражения вредоносными программами, уничтожения данных, проникновения извне или DoS-атак.

Угроза информационной безопасности

Угроза информационной безопасности информационной системы – 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.

- Угроза нарушения конфиденциальности данных включает в себя любое умышленное или случайное раскрытие информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую.
- Угроза нарушения целостности включает в себя любое умышленное или случайное изменение информации, обрабатываемой в информационной системе или вводимой из первичного источника данных.
- Потеря доступности данных – отказ в обслуживании, вызванный преднамеренными действиями одного из пользователей, при котором блокируется доступ к некоторому ресурсу со стороны других пользователей.

Безопасность информационной системы

Комплексная система обеспечения информационной безопасности должна строиться с учетом средств и методов, характерных для четырех уровней информационной системы:

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

Источники угроз

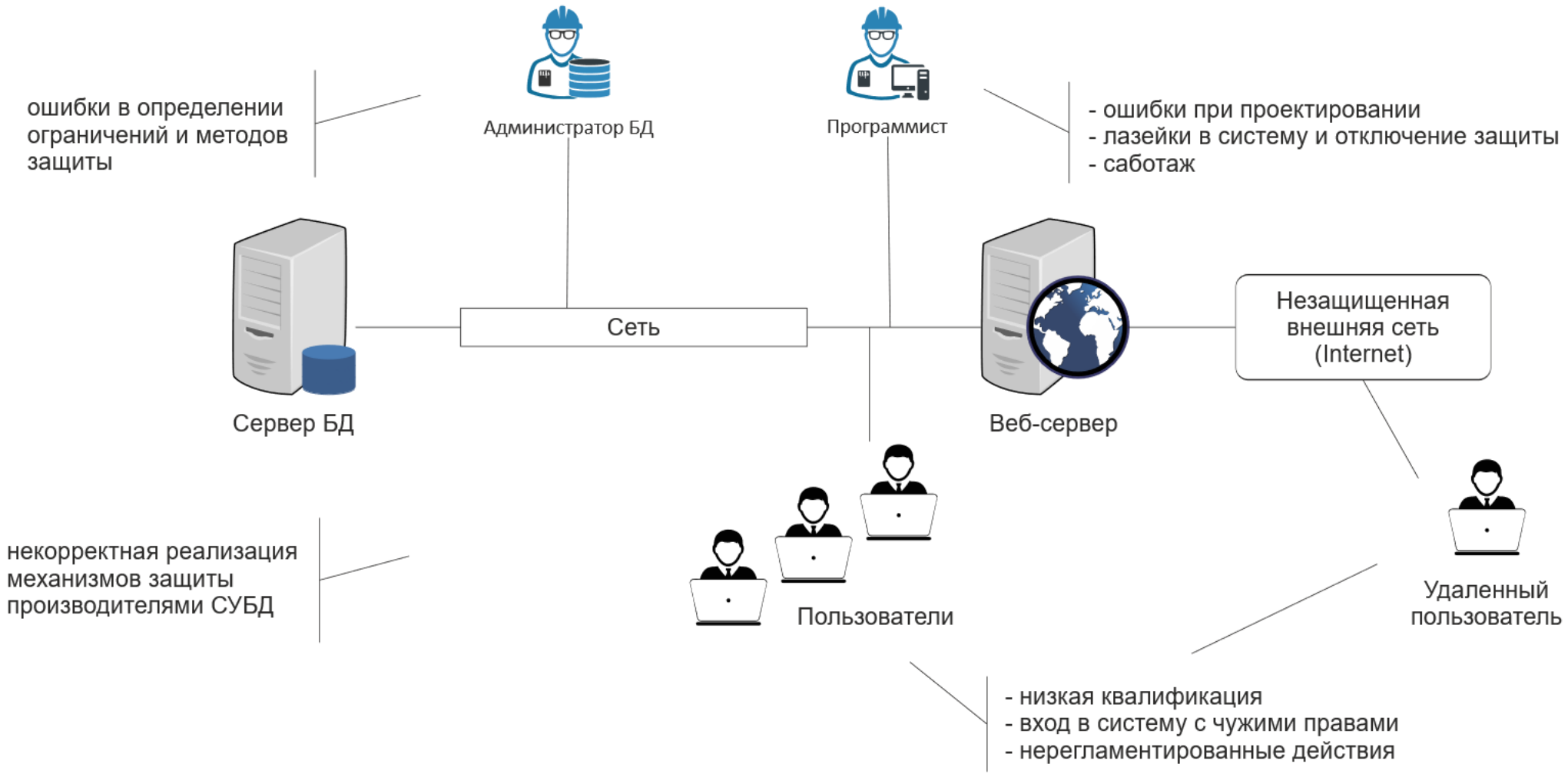
Явные угрозы:

- некорректная реализация механизма защиты;
- некорректная настройка механизма защиты;
- неполнота покрытия каналов доступа к информации средствами защиты.

Скрытые угрозы:

- нерегламентированные действия пользователя;
- ошибки и закладки в программном обеспечении.

Источники угроз



Основные принципы обеспечения безопасности

Основные принципы обеспечения безопасности:

- системность;
- комплексность;
- непрерывность защиты;
- разумная достаточность;
- гибкость управления и применения;
- открытость алгоритмов и механизмов защиты;
- простота применения защитных мер и средств.

Принцип системности

Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности автоматизированной системы.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и получения несанкционированного доступа к информации.

Система защиты должна строиться с учетом не только всех известных каналов проникновения и получения несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности

Комплексное использование широкого спектра мер, методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Комплексная защита информационной системы должна обеспечиваться физическими средствами, организационными и правовыми мерами и использовать средства защиты, реализованные как на уровне операционных систем, так и на прикладном уровне с учетом особенностей предметной области.

Принцип непрерывности защиты

Защита информации - это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные защищенные системы.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена паролей, обеспечение правильного хранения ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность

Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности.

Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Гибкость системы защиты

Часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем.

Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже автору). Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип простоты применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании.

Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Особенности систем БД как объекта защиты

Отличительной особенностью систем БД от остальных видов прикладного ПО является сочетание в себе хранимых данных (собственно БД) и программ управления (СУБД).

Обеспечение безопасности хранимой информации, в частности, невозможно без обеспечения безопасного управления данными. Исходя из этой концепции, все уязвимости и вопросы безопасности СУБД можно разделить на две категории: **зависимые от данных** и **независимые от данных**.

Уязвимости, независимые от данных (их структуры, организации и т.д.), являются характерными для всех прочих видов ПО. К этой группе можно отнести несвоевременное обновление ПО или наличие неиспользуемых функций.

Зависимыми от данных является большое число аспектов безопасности:

- механизмы логического вывода и агрегирования данных;
- специализированные языки запросов (SQL, CQL, OQL и других);
- наборы доступных пользователю функций (которые, в свою очередь, тоже можно считать операторами запросного языка);
- произвольные функции на языке программирования.

Особенности систем БД как объекта защиты

Независимые от данных требования к безопасной системе БД:

1. **Функционирование в доверенной среде**. Под доверенной понимается информационная среда, интегрирующая совокупность защитных механизмов, которые обеспечивают обработку информации без нарушения политики безопасности.
2. **Организация физической безопасности файлов данных**. Данный вопрос требует более детального изучения, так как применяемые структуры данных в различных моделях данных СУБД могут иметь значение при шифровании и защите файлов данных. В целом вопрос сходен с вопросом физической безопасности любых других файлов пользователей и приложений.
3. **Организация безопасной и актуальной настройки СУБД**. К данному аспекту относятся такие общие вопросы обеспечения безопасности, как своевременная установка обновлений, отключение неиспользуемых модулей или применение эффективной политики паролей.

Зависимые от данных требования безопасности:

4. **Безопасность пользовательского слоя ПО**. К этой категории относятся задачи построения безопасных интерфейсов и вызовов.
5. **Безопасная организация данных и манипулирование ими**. Вопрос организации данных и управления ими является ключевым в системах хранения информации. В эту область входят задачи организации данных с контролем целостности, обеспечение защиты от логического вывода и другие, специфичные для СУБД проблемы безопасности.

Угрозы безопасности БД

1. Несанкционированный доступ к данным, структуре данных или к конфигурации безопасности БД, а также удаление или повреждение данных в результате эксплуатации уязвимостей в клиентских приложениях БД (**администрирование прав доступа, правила написания клиентского ПО**).
2. Несанкционированный доступ к данным, структуре данных или к конфигурации безопасности БД, а также удаление или повреждение данных в результате деятельности уполномоченных пользователей БД (**администрирование прав доступа**).
3. Потеря данных вследствие аппаратных или программных сбоев серверов БД случайного или преднамеренного характера (**резервное копирование данных**);
4. Остановка или значительное снижение производительности сервера БД, приводящие к невозможности использования БД по назначению, вызванное большим количеством активных пользователей или преднамеренными атаками (**репликация данных**, **масштабирование БД**);
5. Снижение производительности сервера БД, приводящие к невозможности использования БД по назначению, вызванное преднамеренными действиями уполномоченных пользователей (**средства мониторинга и протоколирования событий**);
6. Беспрепятственный доступ к данным в случае успешной атаки или хищения (**шифрование критических данных**).

Методы защиты информационной системы, касающиеся администрирования непосредственно СУБД:

- аутентификация и авторизация пользователя;
- криптографическая защита БД;
- резервное копирование данных;
- репликация и балансировка нагрузки;
- аудит событий безопасности БД;
- модернизация системного и прикладного ПО;
- доступ к данным только при посредничестве представлений и хранимых процедур.

Идентификация, аутентификация и авторизация

Любой пользователь (или процесс), получающий доступ к БД, на этапе создания пользовательской сессии подлежит обязательной **идентификации**. Все дальнейшие его действия так или иначе будут требовать предъявления этого идентификатора.

Одним из основных способов обеспечения конфиденциальности и целостности информации в БД выступает механизм аутентификации. **Аутентификация** – это процедура проверки подлинности пользователя (точнее, его идентификатора).

Если пользователь успешно прошел процедуру аутентификации, СУБД осуществляет его авторизацию. **Авторизация** – это процедура предоставления пользователю определенных ресурсов и прав на их использование.

Криптографическая защита

В основе подавляющего большинства криптографических систем данных защитой выступает шифрование. Шифрование – это процесс преобразования открытых данных с использованием специального алгоритма, после чего эти данные не могут быть восстановлены к исходному виду без ключа дешифрования.

Большинство СУБД, помимо шифрования данных в таблицах БД, еще обеспечивает криптографическую защиту учетных записей пользователя, исключающую их кражу

Защищенная СУБД должна уметь шифровать: собственно хранящиеся в ней данные (включая служебную информацию), исходный код запросов, хранимых процедур и триггеров, данные, передаваемые к другим компьютерам по незащищенным каналам.

Резервной копией называют копию данных, которая может использоваться для восстановления данных в случае возникновения ошибки или для восстановления копии БД на другом сервере.

Сценарии полного и неполного протоколирования изменений предполагают ведение резервной копии журналов транзакций (в первом случае туда отображаются все операции с БД, а во втором – наиболее важные). Благодаря журналу транзакций возможно не просто восстановление последнего состояния БД, но и откат от этого состояния к наиболее приемлемой точке.

Резервная копия также должна защищаться. Одним из наиболее надежных способов защиты может стать шифрование данных при создании резервных копий.

Репликация и балансировка нагрузки

Серверы баз данных могут работать совместно для обеспечения возможности быстрого переключения на другой сервер в случае отказа первого (отказоустойчивость) или для обеспечения возможности нескольким серверам БД обрабатывать один набор данных (балансировка нагрузки).

Репликацией называется набор технологий копирования и распространения данных и объектов баз данных между базами данных и последующей синхронизации баз данных для поддержания их согласованности.

Фактически использование репликации позволяет осуществить хранение копии одних и тех же данных на нескольких физических серверах в одной сети, каждую такую копию называют репликой.

Аудит событий безопасности

Аудит событий безопасности БД представляет собой процесс получения и анализа данных о происходящих в системе событиях и степени их соответствия требованиям к защите данных.

В идеале сбор информации о состоянии системы безопасности БД должен осуществляться непрерывно, для этого многие СУБД автоматически ведут журнал аудита. В журнале содержится:

- описание стандартного набора событий (авторизации пользователя, доступа к тем или иным данным и операций с ними; создания, модификации и уничтожения объектов БД; выполнение нештатных SQL-команд и т. д.);
- настраиваемый перечень атрибутов в отдельной записи журнала аудита (даты и времени события, идентификатор пользователя, имя и сетевой адрес компьютера, описание события, связанные с событием объекты, признак успешного или неудачного завершения события).

Безопасный доступ к данным

Использование **представлений** (view) позволяет ограничить набор атрибутов таблицы и записей, доступных пользователям.

В целях защиты от SQL-инъекций доступ к хранимым в сетевых БД данным должен осуществляться не через динамический SQL, а с помощью **хранимых процедур** (stored procedure).

САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

БЛАГОДАРЮ ЗА ВНИМАНИЕ

Агафонов А.А.
к.т.н., доцент кафедры ГИиИБ