Тема: Классификация угроз в СУБД

Для того чтобы обеспечить определенный уровень безопасности информационных систем, необходимо понять природу возникающих угроз, основные методы, обеспечивающие снижение уровня уязвимости системы или технологии, и стоимость соответствующих решений, соотнесенную с уровнем безопасности, который обеспечивается решением.

Недостаточный уровень осознания лицами, принимающими решения, природы угроз и назначения и характеристик методов обеспечения безопасности приводит к широкому распространению различных заблуждений.

Реализация всестороннего анализа угроз информационной безопасности любого объекта, в том числе и систем баз данных, требует проведения классификации. Научная классификация опирается на анализ предшествующего опыта, объединяет близкие по содержанию случаи в выделенные разделы классификатора. Независимо от принятого подхода к определению безопасности классификация угроз и их источников представляет самостоятельный интерес. Наличие различных классификаций позволяет исследователю не пропустить существенную для конкретной системы угрозу из богатого списка угроз информационной безопасности баз данных.

Проблема обеспечения информационной безопасности баз данных является многогранной. Сами базы данных — это модель реального мира, который бесконечно многообразен. Проектирование и сопровождение систем баз данных требуют современных программно-аппаратных средств обработки данных и достаточно сложных схем и структур организационного управления. Поэтому можно выбрать много оснований для классификации угроз информационной безопасности баз данных. Учитывая высокий темп изменений в компьютерной и телекоммуникационной индустрии, следует ясно понимать, что вряд ли представленная классификация является исчерпывающей.

Анализ современной научной литературы позволил выделить следующие варианты классификации возможных угроз нарушения информационной безопасности баз данных.

**Классификация по цели реализации угрозы:**

1.  Нарушение конфиденциальности информации, т. е. использование информации, хранящейся в системе, лицами или процессами, которые не были определены владельцами информации.

2.  Нарушение целостности информации, т. е. модификация или уничтожение информации для ее обесценивания путем утраты соответствия с состоянием моделируемых сущностей реального мира.

3.  Полное или частичное нарушение работоспособности системы за счет вывода из строя или некорректного изменения режимов работы компонентов системы, включая их модификацию или подмену.

**Классификация по природе возникновения угрозы:**

1.  Естественные угрозы—угрозы, вызванные воздействием на систему баз данных и ее компоненты объективных физических процессов или стихийно развивающихся природных явлений.

2.  Искусственные угрозы — угрозы информационной безопасности систем баз данных, связанных с деятельностью человека.

**Классификация по локализации источника угрозы представляется следующим образом:**

1.  Угрозы, непосредственным источником которых является человек:

     разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, электронных замков и т. п.) легальными пользователями системы;

     подкуп или шантаж обслуживающего персонала или пользователей, имеющих необходимые полномочия, с целью получения их параметров для процедур аутентификации;

     копирование конфиденциальных данных легальным пользователем системы с целью неправомерного использования (продажа, шантаж и т. п.);

     взлом системы защиты с целью выполнения деструктивных действий лицом, не являющимся законным пользователем системы;

     внедрение агентов фирм-конкурентов или преступных организаций в обслуживающий персонал атакуемой информационной системы (в том числе в административную группу, в группу обеспечения информационной безопасности).

2.  Угрозы, непосредственным источником которых являются штатные программно-аппаратные средства информационной системы:

     неквалифицированное использование или ошибочный ввод параметров программ, способных привести к полной или частичной потере работоспособности системы (аварийное завершение системных процессов, нецелевое расходование вычислительных ресурсов и т. п.);

     неквалифицированное использование или ошибочный ввод параметров программ, способных привести к необратимым изменениям в системе (инициализация баз данных, форматирование или реструктуризацию носителей информации, удаление данных и т. п.);

     отказы и сбои в работе операционной системы, СУБД и прикладных программ.

3.  Угрозы, непосредственным источником которых являются несанкционированно используемые программно-аппаратные средства:

     нелегальное внедрение и использование программ, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей;

     нелегальное внедрение (из-за халатности легального пользователя) и использование троянских программ, предназначенных для исследования параметров автоматизированной информационной системы, сбора данных, зомбирования компьютера с последующим нецелевым расходованием ресурсов и т. п.;

     заражение компьютера вирусами с деструктивными функциями;

     работа генераторов шума и подобных источников электромагнитного излучения.

4.  Угрозы, непосредственным источником которых является среда обитания:

     внезапное и длительное отключение систем электропитания;

     техногенные и природные катастрофы;

     всплески природных электромагнитных излучений. Классификация по расположению источника угроз. Угрозы, источник которых расположен вне контролируемой зоны места расположения автоматизированной информационной системы:

     нарушение нормальной работы или разрушение систем жизнеобеспечения зданий, в которых расположены технические средства и обслуживающий персонал систему — блокирование физического доступа на объект размещения автоматизированной системы обслуживающего персонала или пользователей;

     нарушение нормальной работы или разрушение внешних каналов связи (проводные линии, радиоканалы, оптоволокно).

5.  Угрозы, источник которых расположен в пределах контролируемой зоны расположения автоматизированной информационной системы, исключая места расположения клиентских терминалов и серверных помещений:

     нарушение нормальной работы или разрушение систем электропитания и водоснабжения помещений, в которых расположены технические средства, обеспечивающие работу автоматизированной системы;

     физическое разрушение линий связи или аппаратуры, обеспечивающей работу информационной системы;

     считывание конфиденциальной информации из аппаратных средств телекоммуникационной или вычислительной техники с использованием перехвата электромагнитных излучений;

     выведения из рабочего состояния обслуживающего персонала (организация саботажа, применение отравляющих веществ, психотропных средств и т. п.).

6.  Угрозы, источник которых имеет доступ к терминальным устройствам автоматизированной информационной системы:

     получение параметров входа в систему и аутентифицирующей информации с использованием видеонаблюдения, клавиатурных закладок и технологий подбора паролей;

     получение параметров входа в систему и аутентифицирующей информации с использованием мошеннических приемов, насилия или угрозы насилия;

     получение возможности несанкционированного входа в систему в период, когда легальный пользователь покинул рабочее место, не завершив сеанс взаимодействия с системой;

     получение конфиденциальной информации из распечаток результатов выполнения запросов и иных выводимых системой данных.

7.  Угрозы, источник которых имеет доступ к помещениям, где расположены серверы автоматизированной информационной системы:

     физическое разрушение элементов серверов и коммутационной аппаратуры;

     выключение электропитания серверов и коммутационной аппаратуры;

     остановка серверных и иных критически важных для функционирования автоматизированной системы процессов;

     уничтожение или модификация критически важных для функционирования автоматизированной системы файлов операционной системы;

     нарушение штатной работы базовой операционной системы, например, за счет запуска процессов, активно расходующих ресурсы системы, критически важных для функционирования операционной системы файлов и т. п.;

     рассылка сообщений, дезорганизующих работу пользователей и обслуживающего персонала системы.

**Классификация по способу воздействия на методы и средства хранения данных информационной системы.**

1.  Угрозы нарушения информационной безопасности данных, хранимых на внешних запоминающих устройствах:

     нарушение конфиденциальности, уничтожение или модификация данных, сохраненных средствами создания резервных копий на магнитных носителях, путем незаконного восстановления баз данных с последующей заменой реальной копии или без таковой;

     нарушение конфиденциальности, уничтожение или модификация данных, созданных штатными средствами ведения журнала изменений баз данных; дискредитация криптографических систем защиты информации путем создания копии носителей ключевой информации;

     создание несанкционированных копий файлов операционной системы, содержащих информацию баз данных для проведения последующего анализа с целью доступа к конфиденциальной информации.

2.  Угрозы нарушения информационной безопасности данных, хранимых в оперативной памяти серверов и клиентских компьютеров:

     изменение информации в оперативной памяти, используемой СУБД для кэширования данных, организации хранения промежуточных результатов выполнения запросов, констант и переменных процессов обработки данных;

     изменение информации в оперативной памяти, используемой операционной системой для кэширования данных, организации многопользовательского режима работы, констант и переменных процессов обработки данных;

     изменение информации в оперативной памяти, используемой прикладными программами в процессе организации и выполнения сессии взаимодействия с сервером баз данных и прослушивающим процессом.

3.  Угрозы нарушения информационной безопасности данных, отображаемой на терминале пользователя или принтере:

     организация имитации процесса установления взаимодействия с сервером (ложной сессии) с целью получения идентификаторов и аутентифицирующей информации пользователей;

     изменение элементов данных, выводимых на терминал пользователя за счет перехвата потока вывода;

     изменение элементов данных, выводимых на принтер за счет перехвата потока вывода.

4.  Классификация по характеру воздействия на информационную систему (целесообразно выделить два варианта):

     активное воздействие, т. е. выполнение пользователем системы баз данных каких-либо действий, выходящих за рамки его обязанностей, предусматривающих взаимодействие с системой, или действия внешнего по отношению к ИС пользователя или процесса, нацеленные на достижение одной или нескольких перечисленных выше целей;

     пассивное воздействие, т. е. наблюдение пользователем значений каких-либо параметров СУБД или системы баз данных, а также различных побочных эффектов и косвенных признаков с целью получения конфиденциальной информации на основе анализа собранных данных.

Проблема обеспечения безопасности баз данных является комплексной. Поэтому в качестве математической модели первого приближения уровень обеспечения информационной безопасности некоторой информационной системы может рассматриваться как многомерный вектор, включающий характеристики нескольких независимых измерений:

     физического;

     технологического;

     логического (процедурного);

     человеческого.

Характеристика физического измерения показывает, насколько эффективно обеспечена физическая защита элементов, образующих техническую основу информационной среды электронного бизнеса. Компьютеры, маршрутизаторы, линии связи должны быть физически недоступны для потенциальных носителей деструктивных воздействий. Экраны мониторов, электромагнитные излучения аппаратуры не должны быть источником конфиденциальной информации.

Характеристика технологического измерения показывает, насколько эффективно обеспечена программно-аппаратная реализация процедур, обеспечивающих требуемый уровень безопасности: аутентификация пользователей, разграничение доступа, обеспечение целостности информационной инфраструктуры и т. п. В значительной степени средствам и методам, характерным для данного измерения безопасности баз данных, посвящен материал данного учебного пособия.

Характеристика логического (процедурного) измерения показывает, насколько адекватны логические основы заложенных в систему механизмов безопасности. Если неправильно определены блоки критически важной информации, то она становится уязвимой не из-за недостатков программно-аппаратного комплекса, а из-за ошибок проектирования системы.

Характеристика человеческого измерения показывает, насколько адекватно поведение людей, отвечающих за безопасность системы. Методики измерения этой характеристики должны быть выбраны из арсенала гуманитарных наук. В любой автоматизированной информационной системе есть люди, обладающие критически важной информацией и отвечающие за безопасность системы. Различные мотивы (алчность, неудовлетворенность чем-либо, тщеславие и т. п.) могут привести к добровольной передаче этой информации злоумышленнику либо к непринятию необходимых мер для эффективного противодействия деструктивному воздействию на систему.

Представленные четыре измерения в некотором смысле ортогональны друг другу. Меры, улучшающие характеристики некоторого измерения, не всегда приводят к повышению безопас- ности системы в целом. Характеристики различных измерений должны быть сбалансированы.