3. Лекция

Технологические аспекты информационной безопасности, языки безопасности баз данных

Технологические аспекты защиты информации;

Практическая реализация политик и моделей безопасности, а также аксиоматических принципов построения и функционирования защищенных информационных систем обусловливает необходимость решения ряда программно-технологических задач, которые можно сгруппировать по следующим направлениям:

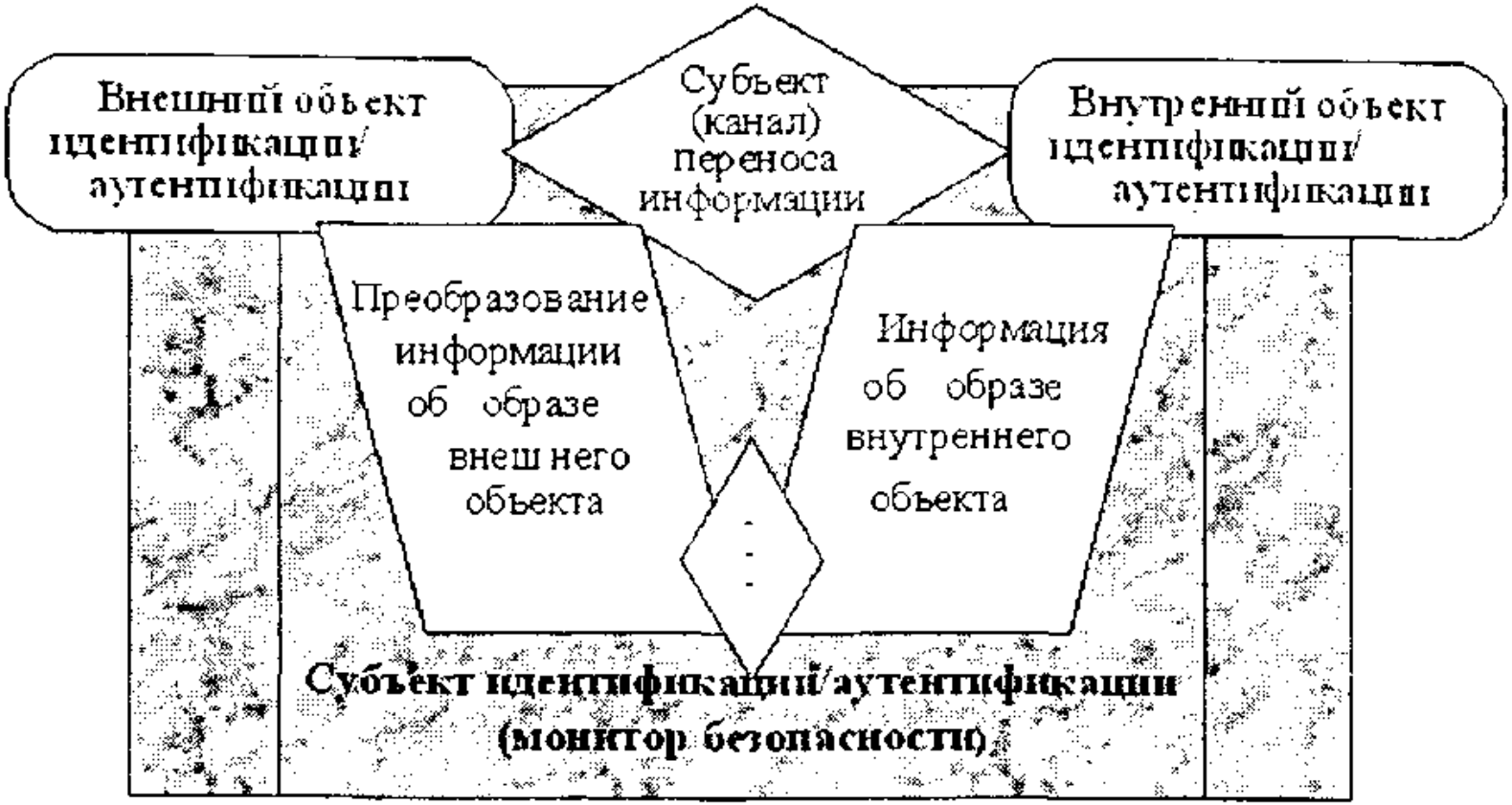
- технологии идентификации и аутентификации;
- языки безопасности баз данных;
- технологии обеспечения безопасности повторного использования объектов;
- технологии надежного проектирования и администрирования.

Идентификация и аутентификация;

Под ***идентификацией*** понимается различение субъектов, объектов, процессов по их образам, выражаемым именами.

Под *аутентификацией* понимается проверка и подтверждение подлинности образа идентифицированного субъекта, объекта, процесса.

В системотехническом плане структуру систем идентификации/аутентификации можно проиллюстрировать схемой, приведенной на рис. 1.5.



необратимому без знания алгоритма и шифра-ключа, т. е. криптографическому, преобразованию и сохраняется в виде ресурса, доступного в системе исключительно монитору безопасности. Таким образом формируется информационный массив внутренних образов объектов идентификации/аутентификации.

Идентификация и аутентификация;

Формирование образов осуществляется на разной методологической и физической основе в зависимости от объекта идентификации/аутентификации (пользователь-субъект; процесс; объект ресурс в виде таблицы, формы, запроса, файла, устройства, каталога и т. д.). В общем плане для идентификации/аутентификации пользователей субъектов в компьютерных системах могут использоваться их биометрические параметры (отпечатки пальцев, рисунок радужной оболочки глаз, голос, почерк и т. д.), либо специальные замково-ключевые устройства (смарт-карты, магнитные карты и т. п.). Однако при доступе непосредственно в АИС (в базы данных), чаще всего используются *парольные системы* идентификации/аутентификации.

Идентификация и аутентификация;

Для аутентификации процессов широкое распространение нашли технологии меток (дескрипторов) доступа.

Технология меток или ***дескрипторов доступа*** отражает сочетание одноуровневой и многоуровневой моделей безопасности данных и основывается на присвоении администратором системы всем объектам и субъектам базы данных специальных дескрипторов доступа, содержащих *набор параметров уровня конфиденциальности, допустимых операциях, допустимых имен объектов или субъектов доступа и других особых условий доступа*. Субъект доступа, *инициируя* в соответствии со своим дескриптором (меткой) разрешенный *процесс,* передает ему свою *метку доступа* (помечает своей меткой). Ядро безопасности СУБД (ТСВ) проверяет ***подлинность метки процесса,*** сравнивая ее с меткой доступа пользователя-субъекта, от имени которого выступает процесс.

При положительном результате метка доступа процесса сравнивается с меткой доступа объекта, операцию с которым намеревается осуществлять процесс. Если дескрипторы доступа процесса и объекта совпадают (или удовлетворяют правилам и ограничениям политики безопасности системы), монитор безопасности разрешает соответствующий доступ, т. е. разрешает осуществление процесса (операции).

Проверка подлинности метки процесса предотвращает возможные угрозы нарушения безопасности данных путем формирования субъектом для инициируемого им процесса такой метки, которая не соответствует его полномочиям.

Идентификация и аутентификация;

Для проверки подлинности меток в системе формируется специальный ***файл (массив) учетных записей.*** При регистрации нового пользователя в системе для него создается учетная запись, содержащая его идентификационный номер (идентификатор), парольный аутентификатор и набор дескрипторов доступа к объектам базы данных (метка доступа). При инициировании пользователем (субъектом) какого-либо процесса в базе данных и передаче ему своей метки доступа ядро безопасности СУБД подвергает метку процесса криптопреобразованию, сравнивает ее с зашифрованной меткой соответствующего субъекта (пользователя) в массиве учетных записей и выносит решение о подлинности метки.

Массив учетных записей, в свою очередь, является *объектом высшей степени конфиденциальности в системе,* и доступен только администратору. Ввиду исключительной важности массива учетных записей для безопасности всей системы помимо шифрования его содержимого принимается ряд *дополнительных мер к его защите,* в том числе специальный режим его размещения, проверка его целостности, документирование всех процессов над ним.

Языки безопасности баз данных

Для определения конкретных назначений или установления правил и ограничений доступа при проектировании банков данных АИС, а также в целях управления системой разграничения доступа и в более широком смысле системой коллективной обработки данных администратору системы необходим специальный инструментарий. Такой инструментарий должен основываться на определенном *языке, позволяющем описывать и устанавливать те или иные назначения доступа и другие необходимые установки политики безопасности в конкретной АИС.*

Языки безопасности баз данных

В реляционных СУБД такой язык должен являться соответственно *составной частью языка SQL*. Исторически впервые подобные вопросы были поставлены и реализованы в упоминавшихся языках SEQUEL (созданного в рамках проекта System R фирмы IBM) и языка QUEL (созданного в рамках проекта INGRES) и послуживших в дальнейшем основой для языка SQL.

Языки безопасности баз данных

Базовых инструкций языка SQL представлены инструкции *GRANT* и *REVOKE*, предоставляющие или отменяющие *привилегии пользователям*. Структура инструкции *GRANT* выглядит следующим образом:

---

*GRANT*список_привилегий_через_запятую *ON* ИмяОбъекта

*TO*ИменаПользователей_через_запятую

[*WITHGRANTOPTION*];

где:

список привилегий составляют разрешенные инструкции (операции) над объектом (таблицей) - *SELECT, INSERT, UPDATE, DELETE;*

список пользователей представляется их именами-идентификаторами или может быть заменен ключевым словом *PUBLIC*, которое идентифицирует всех пользователей, зарегистрированных в системе;

директива *WITH GRANT OPTION* наделяет перечисленных пользователей дополнительными особыми полномочиями по предоставлению (перепредоставлению) указанных в списке привилегий-полномочий другим пользователям.

Языки безопасности баз данных

В целом создание системы разграничения доступа через технику представлений является более простым способом, чем непосредственное использование инструкций *GRANT*, и осуществляется в два этапа:

1. Для всех зарегистрированных пользователей в системе с помощью конструкций *CREATE VIEW* создаются свои представления объектов базы данных.

2. С помощью инструкций *«GRANT SELECT ON*ИмяПредставления *TO* ИмяПользователя» созданные представления авторизуются со своими пользователями.

Безопасность повторного использования объектов

Технологии обеспечения безопасности повторного использования объектов направлены на предотвращение *угроз безопасности* от случайного или преднамеренного *извлечения интересующей злоумышленника информации по следам предшествующей деятельности или из технологического «мусора»*.

Безопасность повторного использования объектов

Часть этих технологий реализуются на уровне операционных систем, а часть являются специфическими функциями, осуществляемыми в автоматизированных информационных системах СУБД. Данные технологии условно можно разделить на три группы:

- изоляция процессов;
- очистка памяти после завершения процессов;
- перекрытие косвенных каналов утечки информации.

Безопасность повторного использования объектов

Изоляция процессов является стандартным принципом и приемом обеспечения надежности многопользовательских (многопроцессных) систем и предусматривает выделение каждому процессу своих непересекающихся с другими вычислительных ресурсов, прежде всего областей оперативной памяти. В СУБД данные задачи решаются мониторами транзакций.

Безопасность повторного использования объектов

Очистка памяти после завершения процессов направлена непосредственно на предотвращение несанкционированного доступа к конфиденциальной информации после завершения работы процессов с конфиденциальными данными уполномоченными пользователями. Так же как и изоляция процессов, чаще всего данная функция выполняется операционными системами. Кроме того, следует отметить, что очистке подлежат не только собственно участки оперативной памяти, где во время выполнения процессов размещались конфиденциальные данные, но и участки дисковой памяти, используемые в системах виртуальной памяти, в которых или операционная система, или сама СУБД АИС временно размещает данные во время их обработки.

Безопасность повторного использования объектов

Как уже отмечалось, при реализации систем разграничения доступа возможны ***косвенные*** *каналы утечки информации*. Помимо проблем с разграничением доступа на уровне полей, источниками косвенных каналов утечки информации являются еще и ряд технологических аспектов, связанных с характеристиками процессов обработки данных. В этом плане различают косвенные каналы *«временные»* и *«по памяти»*.

Надежное проектирование и администрирование

С целью нейтрализации или снижения вероятности данных угроз применяются ряд организационно-технологических и технических средств, решений, объединяемых в общую группу технологий надежного проектирования и администрирования. Их также условно можно разделить на следующие подгруппы:

- технологии надежной разработки программного обеспечения;
- технологии надежного проектирования и создания АИС;
- технические средства и специальный инструментарий администрирования АИС;
- протоколирование и аудит процессов безопасности.