И.А. Ковалькова // Международный менеджмент и маркетинг в сфере образования: материалы четвертой международной научно-практической конференции. – Режим доступа: http://rep.bntu.by/handle/data/35166. – Дата доступа: 03.02.2021.

3. Максименко-Новохрост, Т.В. Цифровая трансформация [Электронный ресурс] / Т.В. Максименко-Новохрост // Государственное управление Российской Федерации: вызовы и перспективы. – Режим доступа: https://bookonlime.ru/product/gosudarstvennoe-upravlenie-rossiyskoy-federacii-vyzovy-i-perspektivy/download – Дата доступа: 17.02.2021.

4. Интегрированная информационная система евразийского экономического союза (интегрированная система) [Электронный ресурс] // Интегрированная система.– Режим доступа: http://system.eaeunion.org. – Дата доступа: 05.03.2020.

УДК 004.056.5

Основные компоненты системы защиты баз данных в СУБД Oracle

Ковалькова И.А., Лабкович О.Н.
Белорусский национальный технический университет

Комплексный подход к защите баз данных (БД) состоит из последовательных этапов, среди них:

– определение адекватной модели угроз;
– оценка рисков;
– разработка системы защиты на её основе с использованием методов, предусмотренных для соответствующего класса информационных систем (ИС);
– проверка готовности систем защиты информации (СЗИ) с оформлением соответствующей документации (описание системы, правила работы, регламенты и т.д.), в том числе заключения о возможности эксплуатации данной СЗИ;
– установка и ввод в эксплуатацию СЗИ;
– учёт применяемых СЗИ, технической документации к ним, а также носителей персональных данных (ПД);
– учёт лиц, допущенных к работе с ПД в ИС;
– разработка полного описания системы защиты ПД;
– контроль использования СЗИ.

Классическая схема защиты баз данных (БД) подразделяется на следующие обязательные процедуры:

• *Разграничение доступа* – каждый пользователь, включая администратора, имеет доступ только к необходимой ему согласно занимаемой должности информации.

• *Защита доступа* – доступ к данным может получить пользователь, прошедший процедуру идентификации и аутентификации.

• *Шифрование данных* – шифровать необходимо как передаваемые в сети данные для защиты от перехвата, так и данные, записываемые на носитель, для защиты от кражи носителя и несанкционированного просмотра/изменения средствами системы управления БД (СУБД).

• *Аудитдоступа к данным* – действия с критичными данными должны протоколироваться. Доступ к протоколу не должны иметь пользователи, на которых он ведётся. В случае приложений, использующих многозвенную архитектуру, приведённые функции защиты также имеют место, за исключением защиты данных на носителе – эта функция остаётся за БД. [1]

Всеми перечисленными функциями безопасности в той или иной мере оснащены СУБД и приложения Oracle. Рассмотрим эти функции подробнее.

1. Разграничение доступа

Преследуя цель защиты БД от инсайдерских угроз, для обеспечения разграничения доступа в версии СУБД 10g Release 3 компания Oracle выпустила новый продукт Database Vault, предназначенный для предотвращения несанкционированного доступа к информации пользователей, в том числе наделённых особыми полномочиями, например, администраторов базы данных. Набор правил в Database Vault, разграничивающих доступ, достаточно широк. Например, руководство организации может определить правила, согласно которым для решения задач, предполагающих доступ к критичной информации, потребуется одновременное присутствие двух сотрудников. Таким образом, Database Vault решает следующие проблемы:

– ограничение доступа к данным администратора БД и других привилегированных пользователей;

– предотвращение манипулирования с базой данных и обращения к другим приложениям администратора приложений;

– обеспечение контроля над тем, кто, когда и откуда может получить доступ к приложению.

2. Защита доступа

Аутентификация в контексте Oracle означает проверку подлинности – пользователя, приложения, устройства, кому или чему требуется доступ к данным, ресурсам или приложениям. После успешной процедуры аутентификации следует процесс авторизации, предполагающий назначение определённых прав, ролей и привилегий для субъекта аутентификации.

Oracle предоставляет разнообразные способы аутентификации и позволяет применять один или несколько из них одновременно. Общим для всех этих способов является то, что в качестве субъекта аутентификации используется имя пользователя. Для подтверждения его подлинности может запрашиваться некоторая дополнительная информация, например, пароль. Аутентификация администраторов СУБД Oracle требует специальной процедуры, что обусловлено спецификой должностных обязанностей и степенью ответственности этого сотрудника. Программное обеспечение Oracle также зашифровывает пароли пользователей для безопасной передачи по сети. [2]

3. Шифрование данных

Для защиты данных, передаваемых в сети, в СУБД Oracle, начиная с версии 8i**,** используется возможности опции Oracle Advanced Security**,** в которой предусмотрена функция Network encryption, позволяющая шифровать весь поток данных. Безопасность информации обеспечивается секретностью ключа, которым шифруются данные.

4. Аудит доступа к данным

СУБД Oracleимеет мощные средства аудита действий пользователей, включающих как доступ к данным, так и события регистрации/выхода и изменения структуры БД. Начиная с версии 9i, СУБД оснащается опцией подробного аудита (Fine Grained Audit Control), которая позволяет проводить аудит доступа по условиям, определяемым достаточно гибкими настраиваемыми правилами. Однако, данные средства аудита не позволяют проследить за действиями, которые совершаются администратором базы данных, а также не мешают ему изменять журнал аудита, удаляя любые строки и не оставляя следов подобных действий. Возникшая необходимость аудита деятельности и защиты данных аудита от привилегированных пользователей, включая администраторов БД, побудило Oracleразработать новую концепцию аудита. В её основу положена идея, на которой базируется функционал *Database Vault*, когда администратор БД изолирован от управления аудитом, что обеспечивает более высокий уровень безопасности БД. Как и в случае Database Vaultправила назначения аудита в Audit Vaultочень гибкие. [3]

Литература

1. Искусство управления информационной безопасностью. [Электронный ресурс]. – http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/obespechenie-zaschity-personalnyh-dannyh-v-subd-oracle.

2. Обзор технологий идентификации и аутентификации. [Электронный ресурс]. – http://www.infosecurity.ru/cgi-bin/mart/.

3. 10 шагов к обеспечению защищенности базы данных Oracle встроенными механизмами безопасности. [Электронный ресурс]. – https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/326445.php

УДК 004.056.5

Современные технологии аутентификации пользователей

Ковалькова И.А., Лабкович О.Н.
Белорусский национальный технический университет

Современная цифровая глобализация привела к возможности получать, хранить и передавать информацию без ограничений, но в то же время, большая часть этой информации нуждается в защите. Одним из самых важных видов защиты информации является ограничение доступа. В данном случае доступ получают те, кто имеет на это право, и это право может быть доказано посредством владения «ключом» – неважно, пароль это, или радужная оболочка глаза. [1]

Здесь необходимо обратиться к понятию аутентификации.

Аутентификация – это процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В зависимости от степени доверительных отношений, структуры, особенностей сети и удалённостью объекта проверка может быть односторонней или взаимной. В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения («да» или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдаёт, с другой стороны – для защиты трафика обмена «субъект - система» от злоумышленника. [2]

Существует очень большое количество технологий аутентификации, и все они обладают разной степенью удобства и надёжности. Основной