Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Аннотация: *в данной работе исследователем рассматриваются основные принципы обеспечения информационной безопасности баз данных.*

Ключевые слова: *информационная безопасность, СУБД, принципы, данные, базы данных.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

Определение 2. Информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Введение

На сегодняшний день разработка универсальной защищённой системы баз данных вероятнее всего является нереальной задачей. При любом разумном методе оценки уровня защищённости этот уровень будет пропорционален затратам на создание системы защиты. Поэтому на практике при ограничении на бюджет системы защиты имеется и определённый предельный уровень безопасности информационной системы, который теоретически можно достичь.

В данное время не существует общепринятой методологии разработки защищённых автоматизированных информационных систем и, в конкретном случае, систем баз данных. Как правило, используется подход, который основан на

анализе лучшего мирового опыта решения проблем данного класса и формулировании основных принципов построения систем, объединяющих накопленный опыт.

Основные принципы

На основе анализа наиболее успешных решений в области защиты информационных систем сформулированы некоторые полезные принципы, которые можно использовать при построении систем защиты баз данных:

1. Экономическая оправданность затрат на механизмы защиты – предписывает применять наиболее простой из возможных вариантов проекта, обеспечивающего достижение поставленной цели. Строгое соблюдение данного принципа позволяет применять на практике методы тщательной проверки кода программных средств и физической проверки аппаратных средств, которые реализуют механизмы защиты.

2. Согласно принципу открытого проектирования, технологии систем защиты не должны основываться на «секретных» алгоритмах. Использование алгоритмов, которые базируются на открытых стандартах в области информационной безопасности, повышает доверие пользователей к системе защиты.

3. Принцип распределения полномочий заключается в том, что необходимо использовать многокомпонентные схемы доступа к информации для критически важных приложений. Например, для выполнения соответствующей операции следует провести аутентификацию её обязательных участников. Следует отметить, что использование многокомпонентных процедур требует больших затрат и могут возникнуть трудности с управлением ключами.

4. В соответствии с принципом минимально возможных привилегий для пользователей и администраторов необходимо, чтобы пользователь (процесс) системы для выполнения конкретной функции использовали наименьший из возможных набор привилегий. Целью данного принципа является минимизация ущерба, возможного в случае ошибки программного обеспечения, сбоя или компрометации элементов системы защиты.

5. Принцип уязвимости системы при отказах и сбоях предписывает осуществлять проектирование информационной системы, реализованной на основе СУБД, с учётом возможности ошибки операционной системы и СУБД, а так же сбоя аппаратуры. При разработке процедур и функций должна выполняться обработка исключительных ситуаций, при обработке конфиденциальной информации необходимо минимизировать риски восстановления информации по содержимому временных файлов и дампам оперативной памяти и т. п.

6. Принцип психологической приемлемости работы средств защиты данных нацелен на улучшение взаимодействия людей с системой защиты. Пользователи должны автоматически и шаблонно использовать имеющиеся механизмы защиты. Слишком сложные механизмы защиты могут вызывать внутреннее неприятие и побуждать к применению скрытого саботажа в различных формах. Принцип психологической приемлемости играет большую роль при выборе модели управления доступом и процедур аутентификации.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

2. Дейт К.Дж. Введение в системы баз данных. – 8-е изд. – М.: Вильямс, 2005. – 1328 с.