Швейкин Владислав Витальевич
студент
Завгородний Станислав Дмитриевич
студент
ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»
г. Самара, Самарская область

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Аннотация: *в данной статье рассматриваются основные особенности и свойства обеспечений безопасности информационной системы и в частности баз данных.*

Ключевые слова: *информационная безопасность, базы данных, конфиденциальность, целостность, доступность, аудит, СУБД.*

Введём некоторые определения, которые будут использованы в работе.

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

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

На сегодняшний день в большинстве случаев основой автоматизированных систем информационного обеспечения управления являются системы управления базами данных. При разработке решения пользователь описывает свои информационные потребности на доступном ему языке. Существующие технические средства могут воспринимать только язык детальных инструкций, поэтому необходимо средство обработки информации, которое обеспечит взаимодействие между пользователем и системой на приемлемом языковом уровне. Так же необходимы инструменты, которые обеспечат разработчику системы доступный

языковой уровень описания технологических процессов обработки данных. Данные задачи могут быть решены с помощью средств современных СУБД.

В настоящее время уровень развития распределённой обработки данных характеризуется размещением логически единой информационной базы в распределённой сетевой среде, многопользовательской обработкой и развитыми средствами разграничения доступа. Вместе с тем реальная структура организации управления доступом должна быть не видна пользователю, а логическое пространство баз данных – единым.

Механизм обеспечения безопасности данных не должен снижать функциональность систем, практически не должен усложнять работу пользователя в системе, а так же обладать гибкостью и удобством администрирования системы.

Можно выделить три основные свойства системы, которые необходимо поддерживать с учётом имеющихся ограничений на используемые ресурсы, для обеспечения информационной безопасности системы:

Конфиденциальность: обеспечение защиты от несанкционированного доступа к данным пользователей, не имеющих явного или неявного разрешения на доступ. Разрешение на доступ к информации определяется внешними по отношению к системе факторами. Система должна иметь языковые инструменты для описания правил, которые определяют возможность доступа к данным. Как правило, предполагается, что используемые правила должны обеспечивать однозначное решение о разрешении или запрещении доступа к информации.

Целостность: защита от преднамеренного или непреднамеренного изменения информации или процессов её обработки. Изменение или уничтожение данных может быть следствием неблагоприятных факторов внешней среды, действий пользователей и проблем, возникающих при параллельной обработке данных в системе.

Доступность: предоставление доступа к информации авторизованным в системе пользователям, в соответствии с принятой технологией. Причиной отказа

в доступности может являться перегрузка системы, вызванная как атаками на систему со стороны злоумышленников, так и объективными причинами, связанными с работой системы.

Одной из важнейших частей обеспечения безопасности информационной системы является регистрация различных событий в системе – аудит. В современном мире не существует абсолютно защищённых информационных систем, а так же нельзя исключить факт возникновения обстоятельств, приводящих к разрушению данных конкретной системы. Профессиональный аудит обеспечивает непрерывный контроль событий, происходящих с базами данных, и является эффективным средством повышения качества информационной безопасности системы. Анализируя данные мониторинга состояния системы, можно определить потенциально опасные для безопасности события или действия пользователей и реализовать процедуры необходимые для предотвращения подобных ситуаций.

Список литературы

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