УДК 004.056.5

Д.Д. Левченко

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Главной идеей статьи является защита данных от несанкционированного доступа. В работе были рассмотрены проблемы безопасности, а также проанализированы основные угрозы для баз данных. В работе упоминается о политики безопасности, которая определяет какие виды информации не должны быть общедоступными. В статье проведен анализ моделей безопасности баз данных, которые формулируют политику безопасности.

Ключевые слова: *база данны, политика безопасности, модель безопасности, доступность, целостность, дискриционная модель, мандатная модель.*

Введение

Актуальность. Термин «база данных» (БД) очень популярен сегодня. Информация, которая хранится в базах данных часто рассматривается в качестве ценного и важного корпоративного ресурса. Многие организации стали настолько зависимы от надлежащего функционирования их систем, что нарушение службы или утечки хранимой информации может вызвать непредвиденные последствия. Корпоративные данные могут относиться к финансовым отчетам, другие могут иметь важное значение для успешного функционирования организации, могут представлять коммерческую тайну, или может описать информацию о лицах, чья частная жизнь должна быть защищена. Таким образом, общая концепция безопасности баз данных является весьма обширной и влечет за собой морально-этические проблемы государства и общества, юридические вопросы управления законодательством над сбором и разглашением хранимой информации, или более технические аспекты, например, как защитить сохраненную информацию от потери или несанкционированного доступа, уничтожения, использования, модификации или разглашения.

Анализ литературы [1-10] показал, что безопасность БД не может рассматриваться как изолированная проблема, поскольку она осуществляется также другими компонентами компьютерной системы. Потребность в безопасности системы определяются с помощью политики безопасности, которая затем обеспечивается различными механизмами безопасности.

Целью данной статьи является анализ угроз и моделей безопасности баз данных.

Основная часть

Безопасность баз данных. Безопасность баз данных является весьма широкой областью, которая решает многие проблемы, в том числе следующие:

– Правовые и этические проблемы, касающиеся права на доступ к определенной информации. Некоторые данные могут считаться приватными и не могут быть доступными на законном основании посторонними лицами. В Соединенных Штатах, существуют многочисленные законы, регулирующие конфиденциальность информации:

– вопросы политики безопасности как на государственном, институциональном, так и на корпоративном уровне, определяют какие виды информации не должны быть общедоступными, например, кредитные рейтинги и личные медицинские записи;

– проблемы, относящиеся к системе, такие как уровни системы, при которой различные функции обеспечения безопасности должны быть приведены в исполнение, например, должна ли функция безопасности обрабатываться на физическом или аппаратном уровне обеспечения, на операционном системном уровне или DBMSlevel;

– необходимость в некоторой организации выявления многоуровневой безопасности, а также для категоризации данных и пользователей на основе этих классификаций, например, совершенно секретно, секретно, конфиденциально и несекретные. Политика безопасности организации в отношении обеспечения доступа к различным классификациям данных должно быть приведена в исполнение. [1]

Угрозы безопасности баз данных. Угрозы для баз данных в результате потери или деградации некоторых или всех из следующих целей безопасности: целостность, доступность и конфиденциальность.

– потеря целостности: целостность базы данных означает требование о том, что информация будет защищена от неправильной модификации. Модификация данных включает в себя создание, вставку, изменение, изменение состояния данных и удаление. Целостность теряется, если данные несанкционированно изменены. Если установленная потеря системы или целостность данных не будет исправлена, то дальнейшее использование зараженной системы или искаженных данных может привести к неточности, мошенничеству или неправильным решениям;

– потеря доступности: доступность базы данных относится к созданию объектов, доступных для

пользователя или программы, на которые они имеют законное право;

– потеря конфиденциальности: конфиденциальность базы данных относится к защите данных от несанкционированного раскрытия. Последствием несанкционированного раскрытия конфиденциальной информации может варьироваться от нарушения закона о конфиденциальности данных до обеспечения национальной безопасности. Несанкционированные, непредвиденные или непреднамеренное разглашение могут привести к потери доверия населения, смущение, или судебный иск против организации [10].

Цель политики безопасности баз данных. Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса.

После того как политика безопасности определена, должен решаться вопрос о технологии ее реализации в автоматизированном контуре. Для реализации сформулированных в терминах естественного языка правил и норм политики безопасности необходимо использовать (или разработать) некоторую формальную модель, которая допускает эффективное программирование на каком-либо формальном языке [9].

Целью формализации политики безопасности для информационной системы является четкое изложение взглядов руководства организации на существо угроз информационной безопасности, организации и технологий обеспечения безопасности ее информационных ресурсов. Политика безопасности обычно состоит из двух частей: общих принципов и конкретных правил работы с информационными ресурсами и, в частности, с базами данных для различных категорий пользователей [7].

Наличие политики безопасности поможет управлять бизнес-процессами, очертит объекты, нуждающиеся в защите, и заложит прочную основу для реализации компенсирующих элементов контроля. Успех программы по ведению журнала безопасности и мониторингу базы данных зависит от целей и имеющихся нормативов. Во-первых, понимание задач бизнеса, законов, правил и ресурсов, необходимых для защиты компании поможет разработать эффективную политику безопасности, а также базовые бизнес-процессы на основе все этой информации. Как упоминалось ранее, эта предварительная работа имеет критически важное значение, но часто упускается многими компаниями. Однако закладка фундамента не гарантирует успешности всей кампании, а только подготовит организацию к работе по построению успешной программы. [9]

Модели безопасности БД. Из-за разнообразия доменых приложений для баз данных, различных моделей и методов защиты, были предложены модели безопасности для борьбы с различными угрозами.

Модель безопасности это формальное выражение и формулирование политики безопасности.

Модель безопасности включает в себя:

– модель информационной системы;

– принципы, критерии, целевые функции и ограничения защищенности данных от угроз;

– ограничения, алгоритмы, формализованные правила, механизмы и схемы безапосного функционирования системы. [8]

Большинство моделей безопасности основывается на субъектно-объектной модели компьютерных систем, в том числе и баз данных.

Простейшая одноуровневая модель безопасности на основе дискреционного принципа разграничения доступа безопасности являются фундаментальными для операционных систем и СУБД (систем упраления базами данных). Однако, появление более продвинутых моделей данных не имеет повышенный интерес к дискреционной политики. [4]

Дискреционная политика безопасности. Дискреционная политика безопасности - политика осуществляемая на основании заданного администратором множества разрешенных отношений доступа. Дискреционное управление доступом определяется двумя свойствами:

– все субъекты и объекты должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Дискреционная безопасность обеспечивается в большинстве коммерческих СУБД и базируется на концепции представлений базы данных. Вместо того, чтобы разрешать пользователю базовые отношений с системой информационной матрицы контроля доступа, которая предназначена для ограничения доступа пользователя к определенному подмножеству данных [2, 4].

Мандатная модель безопасности. Мандатная политика безопасности – политика, основанная на совокупности предоставления определенного доступа, на множестве атрибутов безопасности субъекта и объекта. Мандатная политика решает более высокий уровень угрозы, чем дискреционная политика, потому что в дополнение к управлению доступом к данным, они могут также управляют потоком данных. Кроме того, мандатные методы защиты преодолеть структурные ограничения защиты основанные на DAC [2, 4]. Основу мандатной политики безопасности составляет мандатное управление доступом (Mandatory Access Control – MAC).

В то время как дискреционная модели связаны с определением, моделированием, а также обеспечением доступа к информации мандатных моделей безопасности в дополнение к имеющим отношение к потокам информации в системе. Мандатная безопасность требует, чтобы объекты безопасности и субъекты назначаются определенные уровни безопасности, представленных меткой. Меткой для объекта О называется его классификация (class(o)), а метка для субъекта s называется ее разрешением (clear(s)). Классификация отображает чувствительность к меченым данным. Метка защиты состоит из двух компонентов: уровня иерархии секретности или доступа классов и представителя не иерархических категорий. Уровни разрешения и классификация полностью упорядочены в то время как метка безопасности только частично упорядочеа - таким образом, множество классификаций образует решетку [3, 4].

Адаптирование модели мандатного контроля доступа, для большего приспособления к основной цели обработки данных и предлажения конструкции для разработки баз данных, содержащих конфиденциальную информацию, является главной целью адаптированной модели мандатного контроля доступа (AMAC). Для того, чтобы преодолеть ограничения MAC, AMAC предлагает несколько функций, которые помогают проектировщику базы данных при выполнении различных видов деятельности, участвующих в разработке базы, содержащей конфиденциальную информацию. Для AMAC в методике безопасности баз данных существуют следующие преимущества:

– Методика поддерживает все этапы проектирования базы данных и может быть использована для построения защиты дискреционной, а также для построения мандатных защищенных баз данных.

– в случае мандатной защиты требуется вспомогательная политика для выведения фрагментов базы данных обеспечивается целевой защитой;

– в случае мандатной защиты требуется автоматизированной защита маркировки для объектов безопасности и поддерживается субъектами;

– в AMAC безопасность обеспечивается с помощью триггеров базы данных и, при этом, они могут быть доработаны для соответствия требованиям безопасности зависимых приложений. [4, 6]

Модель Кларка и Уилсона. Эта модель была впервые резюмирована и была сравнена с MAC Кларком и Уилсоном в 1987 году. Авторы утверждают, что их модель основана на концепции, которая уже хорошо зарекомендовала себя. Это представление о субъектах и объектах безопасности, набор хорошо сформированных операций и принципов разделения обязанностей. Если перевести эти принципы в мир баз данных и безопасности, то они интерпретируются следующим образом: пользователи системы имеют ограничения только на выполнение определенного набора операций, допустимых им и каждая транзакция работает только на заданном множестве объектов данных. Точнее, подход Кларка и Уилсон интерпретируется следующим образом:

1. Субъектам безопасности назначаются роли. На основе их ролей в организации пользователи выполняют определенные функции. Каждая бизнес-роль отображается в функции базы данных, и в идеале в определенный момент времени конкретный пользователь играет только одну роль. Функция базы данных соответствует набору (wellformed) операций, которые необходимы для пользователей, действующих в роли. В рамках этой модели необходимо указать соответсвие пользователям их ролей и, в какое время, для какой роли, какие транзакции необходимо выполнять. Для того, чтобы контролировать несанкционированное раскрытие и модификация данных Кларк и Уилсон предлагают доступ, который будет разрешен только посредством выполнения определенных программ, wellformed сделок, и что права пользователей на выполнение такого кода будет ограничено в зависимости от роли каждого пользователя.

2. Правильное построение транзакции. Правильно составленная транзакция работает на заданном множестве данных и гарантирует, что все соответствующие свойства безопасности и целостности удовлетворены. Кроме того, она обеспечивает журналирование и атомарность, а также упорядоченность результатов частных операций, таким образом, что параллелизм и механизмов восстановления могут быть установлены. Важно отметить, что в этой модели элементы данных, на которые ссылаются транзакций не задаются пользователями действующей транзакции. Вместо того, элементы данных назначаются в зависимости от той роли, в которой пользователь действует. Таким образом, модель не позволяет специальные запросы к базе данных.

3. Разделение обязанностей. Этот принцип требует, чтобы каждой группе пользователей назначался определенный набор функций в зависимости от роли пользователя в организации. Единственный способ получить доступ к данным в базе данных с помощью заданного набора - это хорошо сформированная транзакция, характерная для роли каждого из пользователей. В тех случаях, когда пользователь запрашивает дополнительную информацию, другой пользователь (который находится на более высоком уровне), действующий в отдельной роли должен использовать wellformed транзакции, который действует из домена транзакций роли, чтобы предоставить временное разрешение пользователю выполнить большой набор корректно сформированных операций. Кроме того, роли должны быть определены таким образом, чтобы не было возможным для одного пользователя нарушить целостность системы. Например, проектирование, внедрение и поддержание корретно сформированных транзакций, должны быть отнесены к другой роли, чем исполнение этих же транзакций. [4, 5]

Выводы

Таким образом, безопасность баз данных не является отдельной проблемой - в самом широком смысле это общая системна проблема. Безопасность баз данных зависит не только от выбора конкретной продукта СУБД или от поддержки определенной модели безопасности, но и от операционной среды, а также вовлеченных людей. Дальнейшие вопросы безопасности базы данных включают в себя требования к операционной системе, сетевой безопасности, дополнительные пакеты безопасности, шифрование данных, безопасность статистических баз данных, аппаратных средств защиты, верификации программного обеспечения и др.

При выборе подхода к обеспечению безопасности дискреционный может быть первым выбором, если высокая степень безопасности не требуется. Сохраняя ответственность за соблюдение безопасности на стороне пользователей, если потенциальные угрозы безопасности не приведет к значительному ущербу.

Мандатные политики являются более эффективными, поскольку они предполагают, что пользователи не имеют контроль над созданием и изменением параметров безопасности. Политика безопасности подходит для конкретного приложения также могут иметь как обязательный и дискреционный компонент. Кроме того, реальные системы часто предлагают утечки на строгих обязательного контроля, например, для привилегированных пользователей, таких как системные администраторы и сотрудников службы безопасности. Такие точки входа часто представляют собой серьезный источник уязвимости. Многоуровневые приложения могут стать очень сложными.

Хотя очень эффективные мандатные политики могут применяться только в средах, где доступна метка информации. Это считается одним из самых сильных пунктов в пользу модели безопасности AMAC. AMAC предлагает среду разработки для баз данных с основным акцентом на безопасность. Она включает в себя дискреционное, а также мандатное управление

Модель Кларка и Уилсона получила широкое внимание в последние годы. Многое из защиты соответствующих действий сгенерировано для прикладных программ и моделей не поддерживают специальные запросы к базе данных. В частности авторы ссылаются на потенциальные угрозы безопасности системы таких, как распространение данных, несанкционированные действия и злоупотребление привилегиями со стороны авторизированных пользователей.

Список литературы

1. Elmasri, Ramez. Fundamentals of database systems / Ramez Elmasri, Shamkant B. Navathe.--4th ed. – Pearson. Additson Wesley, 2003. – 1029p. – ISBN 0-321-12226-7.

2. Fernandez, E., Summers, R., and Wood, C. [1981] Database Security and Integrity, Addison-Wesley, 1981.

3. Günther Pernul. Database Security. - Vienna, Austria, 1994. – 75 p.

4. Meg Coffin Murray. Database Security: What Students Need to Know/ Meg Coffin Murray. Journal of Information Technology Education: Innovations in Practice, 9, 2010 – P. 61-77

5. Защищеныые системы – общие принципы [Электронный ресурс]. Режим доступа : http://crypto.pp.ua/2010/06/319/

6. Информационная безопасность в современных системах управления базами данных [Электронный ресурс]. Режим доступа : http://compress.ru/article.aspx?id=10099

7. Общие сведения о параметрах политики безопасности [Электронный ресурс]. Режим доступа - https://technet.microsoft.com/ru-ru/library/hh831424(v=ws.11).aspx

8. Понятие и модели безопасности данных [Электронный ресурс]. Режим доступа : http://www.razgovorodele.ru/moresec/materials13/automated_control_systems_7/adm_systems04.php

9. Разработка политики безопасности [Электронный ресурс]. Режим доступа - http://sernam.ru/ss_31.php

10. Угрозы безопасности информации. Угрозы конфиденциальности, целостности доступности АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности. [Электронный ресурс]. Режим доступа – http://ofsky0.narod.ru/17.htm.

Надійшла до редколегії 3.02.2017

Рецензент: д-р техн. наук, проф. А.В. Горбенко, Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків.

АНАЛІЗ ПОЛІТИКИ ТА МОДЕЛЕЙ БЕЗПЕКИ БАЗ ДАННИХ

Д.Д. Левченко

Головною ідеєю даної статті є захист даних від несанкціонованого доступу. У роботі були розглянені роблеми безпеки, а також проаналізовані загрози для баз даних. У роботі згадується про політику безпеки, яка визначає які види інформації не повинні бути загальнодоступними. У статті проведено аналіз моделей безпеки баз данних, які формулюють політику безпеки.

Ключові слова: *база даних, політика безпеки, модель безпеки, доступність, цілісність, дискриціонна модель, мандатна модель.*

ANALYSIS OF SECURITY POLICIES AND MODELS DATABASE SECURITY

D.D. Levchenko

The main idea of the article is to protect data from unauthorized access. In this work we were considered security concerns, and the analysis of the main threats to the database. The paper refers to the security policy, which defines the type of information that should not be publicly available. The article analyzes the database security model data to formulate a security policy.

Keywords: *data base, security policy, security model, availability, integrity, discretionally model credentials model.*