УДК 004.942

В.В. Баранов[2], М.А. Бирюков[1], С.А. Кравченко[2],
А.С. Максимов[2], И.Б. Саенко[1]

[1]Россия, г. Санкт-Петербург, Военная академия связи им. С.М. Буденного
[2]Россия, г. Новочеркасск, Южно-Российский государственный
политехнический университет имени М.И. Платова

ИМИТАЦИОННАЯ МОДЕЛЬ ДЛЯ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОЕКТИРОВАНИИ РОЛЕВЫХ СХЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА К БАЗАМ ДАННЫХ

В статье проанализированы источники угроз информационной безопасности баз данных, использующих ролевую модель распределения 26ннтупа. Рассмотрены вопросы построения имитационной модели для анализа рисков информационной безопасности ролевых базы данных. Проведена оценка рисков информационной безопасности ролевых баз данных с использованием разработанной модели.

Ключевые слова: имитационная модель, база данных, ролевая модель разграничения доступом, информационная безопасность.

Введение

Защита баз данных от несанкционированного доступа является одной из важнейших проблем в области информационной безопасности. Известно большое количество публикаций, свидетельствующих о большом количестве фактов несанкционированного доступа к информации, содержащейся в базах данных (БД) [1]. Причем, по оценке специалистов, большой процент случаев несанкционированного доступа остается нераскрытыми. При этом следует отметить, что в условиях реализации современной тенденции к объединению совместно разделяемых ресурсов автоматизированных систем (АС) различного назначения в единое информационное пространство, помимо новых возможностей по повышению совокупной эффективности аппаратного и программного обеспечения и критически важных данных в таких системах появляются риски несанкционированного доступа к информации, содержащейся в БД.

1.Ролевая модель разграничения доступа

Как правило, для реализации политики безопасности единого информационного пространства, в котором функционирует большое количество АС, наиболее эффективно используется ролевая модель контроля доступа (Role-Based Access Control, RBAC) [2]. В модели RBAC администратор безопасности производит формирование и назначение ролей и построение иерархии ролей. В соответствии с назначенными ролями определяются разрешенные полномочия пользователей. Ключевыми достоинствами данной модели являются: легкая управляемость и контролируемость поведения объектов и субъектов в системе; возможности построения иерархий и масштабирования; выражение средствами ролевой модели дискреционную и мандатную модели разграничения доступа, которые получили наибольшее применение в различных автоматизированных системах.

Для проектирования единой модели RBAC, в качестве исходных данных принято принимать:

– $\left|ROLES\right| \to \min$ – множество *пользователей*;

– $PRMS = \{p_j\}, j = 1,...,n, n = \left|PRMS\right|$ – множество *полномочий*;

– $ROLES = \{r_l\}, l = 1,...,k, k = \left|ROLES\right|$ – множество ролей.

– $UA \subseteq U \times ROLES$ – отображения множества пользователей на множество ролей;

– $PA \subseteq PRMS \times ROLES$ – отображение множества полномочий на множество ролей;

– $UPA \subseteq U \times PRMS$ – отображение множества пользователей на множество полномочий.

Следует отметить, что результат последовательного применения друг за другом отображений *UA* и *PA* может отличаться от *UPA*, если ролевая схема имеет некоторые ограничения или она сформирована администратором некорректно. Поэтому для такого отображения принято использовать обозначение *DUPA*, что означает *Direct UPA* (рисунок 1).

Совокупность <*U*, *PRMS*, *ROLES*, *UA*, *PA*> принято называть *конфигурацией*, или *схемой RBAC*, которая обозначается как $ChRD_{адм}$. В дальнейшем будет использоваться второе определение [3].

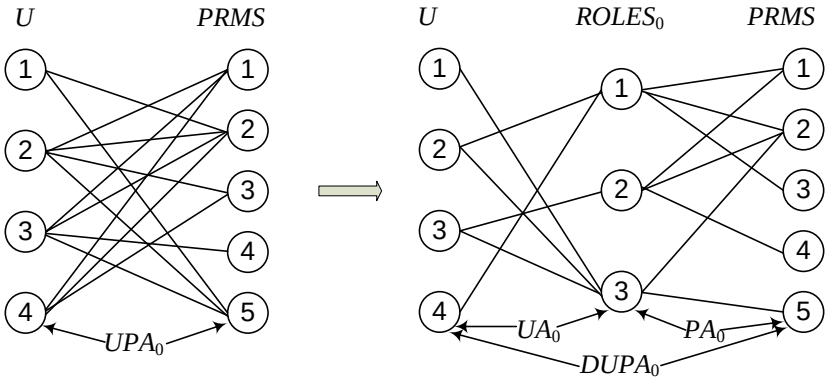

Рисунок 1 – Пример классического определения ролевой модели RBAC

2. Анализ рисков информационной безопасности

В наибольшей степени подвержены воздействию угроз информационной безопасности АС в силовых структурах, особенно угроз разглашения информации, содержащей критически важные сведения. При этом наиболее опасны копирование информации и ее искажение вследствие непреднамеренных, случайных или целенаправленных воздействий.

Наиболее существенными в данной области являются следующие факторы риска нарушения установленных требований по защите информации и ее обработки в АС:

1) большой объем разнородной информации;

2) ценность практический всей информации, хранящийся в БД и циркулирующей во всем пространстве АС;

3) существенный перечень лиц, имеющий доступ к информации;

4) наличие случаев использования несертифицированных технических средств и программного обеспечения;

5) выполнение работ пользователями вне полномочий;

6) отсутствие единого подхода к разграничению доступа;

7) недостатки организационного обеспечения защиты информации, несоблюдение требований по защите информации;

8) ошибки администраторов безопасности.

Наиболее вероятными источниками для нанесения ущерба БД АС, функционирующим в едином информационном пространстве, является внутренний нарушитель. При этом нарушить будет стремиться к сокрытию следов свой деятельности. Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации [4].

3. Имитационная модель учета рисков информационной безопасности

Задача проектирования ролевой схемы разграничения доступа к базе данных заключается в следующем:

– первоначальное проектирование (конфигурация) схемы $ChRD_{\text{адм}}$, удовлетворяющей требованиям по обеспечению безопасного и доступного разграничения доступа к БД вида:

$$ChRD_{\text{адм}} = \langle U, O, R \rangle; \tag{1}$$

– использование $ChRD_{\text{адм}}$ для обеспечения требуемой доступности;

– своевременное реконфигурация схемы $ChRD_{\text{адм}}$ в схему вида:

$$ChRD_{\text{адм}}^{\text{ркфг}} = \left\langle ChRD_{\text{адм}}, U', O', R' \right\rangle, \tag{2}$$

где U', O', R' – множество пользователей, ресурсов и ролей, соответственно, измененные в процессе ее администрирования.

Для принятия решения о реконфигурации схемы разграничения доступа необходимо оценить риски влияния изменений, вносимых администратором безопасности в первичную схему разграничения доступа, и определить достаточные условия реконфигурации.

В качестве показателя критичности рисков предлагается взять «коэффициент ошибки доступа» $K_{\text{ош}}$, который характеризуется вероятностью возникновения отказа в доступе ($P_{\text{НОД}}$) и вероятностью несанкционированного 29ннтупа ($P_{\text{НСД}}$) при единичном воздействии на схему доступа $ChRD_{\text{адм}}$ следующим образом:

$$K_{\text{ош}} = 1 - \left(1 - P_{\text{НСД}}\right)\left(1 - P_{\text{НОД}}\right) \tag{3}$$

Целью моделирования является определение выполнения условий достаточности для выполнения реконфигурации исходной схемы. К схемам разграничения доступа предъявляются требования по доступности, указанные в таблице 1.

Выражения для расчета значений показателей доступности разграничения доступа являются следующими:

$$P_{\text{нсд}} = \frac{N_{\text{ош}}^{\text{дост}}}{N_{\text{общ}}}, \tag{5}$$

$$P_{\text{нод}} = \frac{N_{\text{ош}}^{\text{отк}}}{N_{\text{общ}} - N_{\text{прав}}^{\text{отк}}}, \qquad (6)$$

где $N_{\text{общ}}$ – общее количество запросов доступа,

$N_{\text{ош}}^{\text{дост}}$ – количество ошибочно разрешенных запросов,

$N_{\text{ош}}^{\text{отк}}$ – количество ошибочных отказов в доступе,

$N_{\text{прав}}^{\text{отк}}$ – количество обоснованных отказов в доступе.

Таблица 1 – Показатели доступности

Наименование показателя	Обозначение	Характеристика показателя	Допустимые значения
Вероятность несанкциони-рованного 30ннтупа	$P_{\text{НСД}}$	$P_{\text{НСД}} \le P_{\text{НСД доп}}$ определяет вероятность ошибок 1-го рода	$P_{\text{НСД доп}} = 10^{-3}$
Вероятность необоснован-ного отказа в доступе	$P_{\text{НОД}}$	$P_{\text{НОД}} \le P_{\text{НОД доп}}$ определяет вероятность ошибок 2-го рода	$P_{\text{НОД доп}} = 10^{-2}$

Заключение

Таким образом, достаточным условием принятия решения по реконфигурации схемы разграничения доступа RBAC будет нарушение требований по доступности, приведенных в таблице 1. Результаты моделирования показали, что в БД с большим числом пользователей каждое изменение ролевой модели доступа администратором безопасности может приводить к значительному увеличению ошибок доступа (в среднем 10^{-2}). Следовательно, оценка рисков проектирования ролевой схемы разграничения доступа позволит своевременно провести реконфигурацию, что исключит появление ошибок «ручного» администрирования.

Литература

1. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах// Информация и космос №1 2017 С 121-126.

2. Саенко И.Б., Бирюков М.А. Методика интеграции локальных схем разграничения доступа к разнородным ресурсам единого информационного пространства // Материалы конференции «Информационные технологии в управлении» (ИТУ-2016). – СПб.: АО «Концерн «ЦНИИИ «Электронприбор», 2016. – С.758-762.

3. Saenko, I. Reconfiguration of RBAC schemes by genetic algorithms/ I. Saenko, I. Kotenko // Intelligent Distributed Computing. X. Studies in Computational Intelligence. Springer-Verlag, Vol. 678. Proceedings of 10th International Symposium on Intelligent Distributed Computing – IDC'2016. Paris, France.

4. Авраменко В.С, Козленко А.В. Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю // Труды СПИИРАН. – 2010. - № 2(13). – С. 172-181