УДК 004.056.523:004.4

Бахрачева Ю.С., Евдокимова Е.А.

МОДЕЛЬ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация. Рассмотрена проблема повышения уровня безопасности к объектам в информационной системе с дискреционным разграничением прав доступа. Представлена модель разграничения прав доступа с использованием «пользователя-посредника». Разработан программный комплекс с использованием данной модели для повышения эффективности работы администратора.

Ключевые слова: информационная система, разграничение прав доступа, уровень безопасности информационной системы.

Abstract. The problem of increase of the security level to objects in an information system with discretionary demarcation of access rights is considered. The model of demarcation of access rights with use of «intermediary user» is provided. The program complex with use of the this model is developed for increase of overall performance of the administrator.

Keywords: information system, demarcation of access rights, security level of an information system.

Введение

Механизмы управления доступом являются основой защиты информационных процессов и ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным ресурсам и процессам – объектам [3, 5]. В качестве субъектов в простейшем случае понимается пользователь [4].

Информационные ресурсы представляют собой отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Под информационным процессом будем понимать процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации [1].

Права доступа определяют, какие действия (чтение, запись, выполнение) может выполнять субъект (пользователь системы) над её объектами (ресурсами). Их задание можно осуществить несколькими способами, наиболее распространёнными являются следующие три модели управления правами доступа: дискреционная модель; мандатная модель; ролевая модель.

Во многих случаях модели не используются в чистом виде, а комбинируются между собой.

Модель разграничения прав доступа с использованием «пользователя-посредника»

В данной работе для управления правами доступа предлагается модель с «пользователем-посредником». В случае дискреционной модели описаны права для каждой пары субъект-объект, в таком случае для каждого субъекта будут указаны действия, которые он может осуществлять по отношению к каждому объекту. В новой модели у субъектов не будет никакого доступа к объектам.

К выбранному объекту прикрепляется субъект «посредник» и он и только он имеет право доступа к нему и только к нему. Таким образом, все пользователи получают доступ к объекту только через посредника.

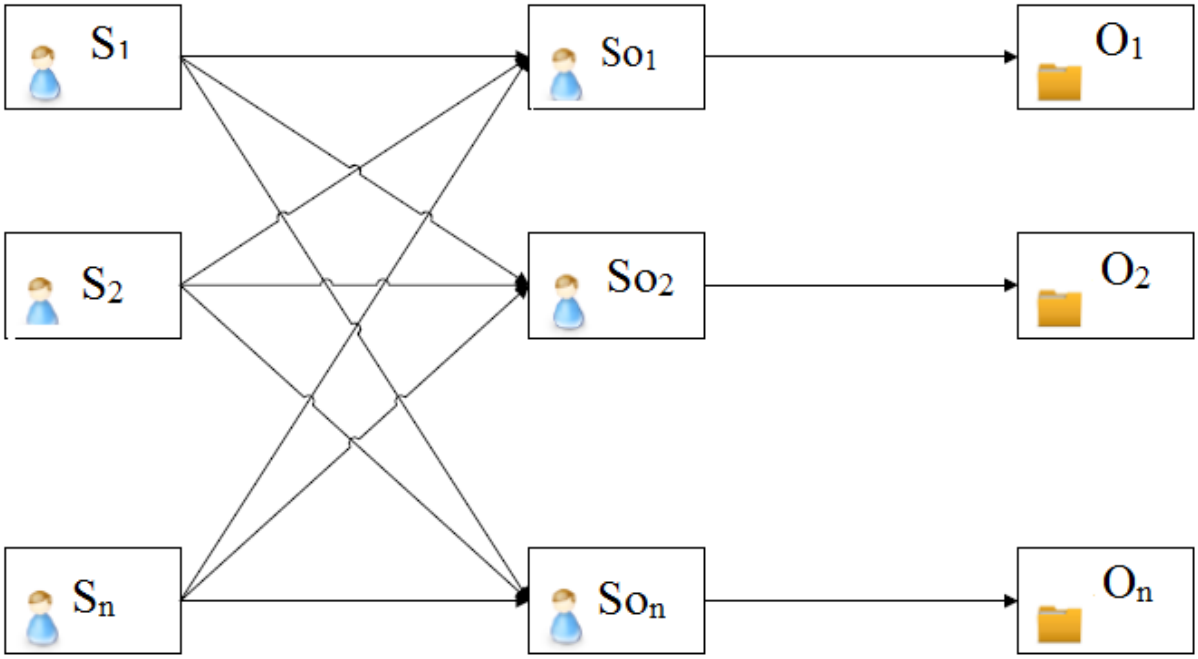

Рисунок 1 – Модель разграничения прав доступа с использованием «пользователя-посредника»

На Рисунке 1 представлено графическое изображение рассматриваемой модели, где: S_n – множество субъектов системы; So_n – множество субъектов посредников; O_n – множество объектов системы.

В результате, если происходит компрометация одного из объектов, то не будет произведена компрометация остальных объектов системы.

Можно сделать следующий вывод, что использование данной модели относительно взятой за основу дискреционной она более эффективно в защите данных системы.

Для повышения эффективности работы администратора, уменьшения времени настройки, приведённой ранее модели, был разработан программный комплекс, реализующий следующие функции:

1) Вывод списка существующих пользователей системы на экран.
2) Вывод существующих на компьютере объектов.
3) Вывод списка прав пользователей к объектам.
4) Возможность изменения прав доступа пользователей к объектам.
5) Возможность создания новых пользователей.
6) Изменение принадлежности пользователей к группам.
7) Вывод факта доступа субъекта к объекту.
8) Возможность просмотра количества фактов доступа субъекта к объекту.

Первые три функции позволяют производить мониторинг прав доступа, функции 4, 5, 6 необходимы для настройки «посредника».

Функции 7, 8 предназначены для построения модели реально необходимых полномочий.

В системах с дискреционным разграничением прав доступа пользователь имеет избыточные права и стоит вопрос предоставления ему прав действительно необходимых для выполнения служебных обязанностей. Решение этой задачи затруднено тем, что пользователи, входящие в определенные группы, могут работать с различными множествами документов и состав этого перечня документов непостоянен во времени.

Рассмотрим, как будет производиться анализ фактов доступа пользователей к объектам, описывающихся в журнале событий ОС Windows:

Введём следующие обозначения: S – субъект (пользователь); O – объект (ресурс); A – право доступа (чтение, запись, выполнение); $R(S,O,A)$ – результат доступа к объекту, принимает значения *allow* и *deny*; FD – факт доступа субъекта к объекту (запись о доступе в журнале событий); p – параметр, описывающий нормальное количество фактов доступа одного субъекта к определённому объекту.

Таким образом, формула, описывающая возможность получения объектом доступа к субъекту имеет следующий вид:

$$R_j = \begin{cases} \sum FD_j \geq p, allow \\ \sum FD_j < p, deny \end{cases}$$

где j – номер ресурса в списке.

Результаты и обсуждение

Определим архитектуру программного комплекса.

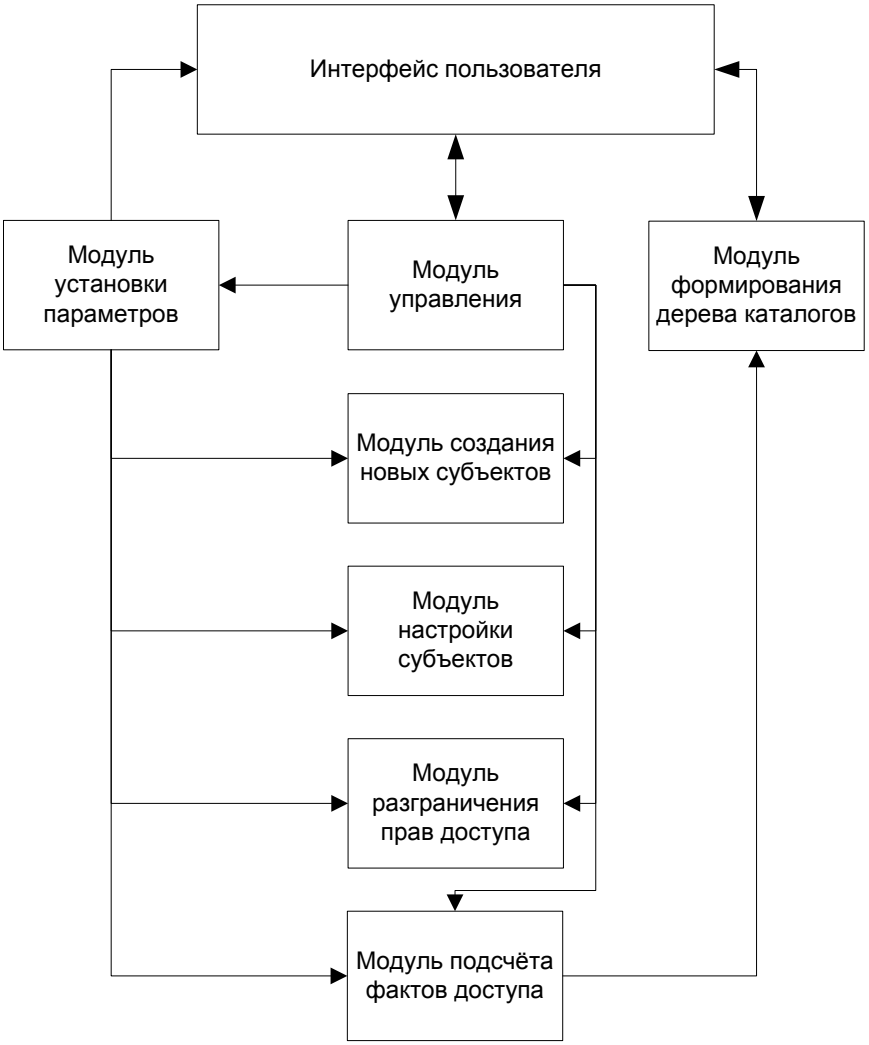

Рисунок 2 – Архитектура программного комплекса

Архитектура, представленная на Рисунке 2, включает в себя следующие модули:

1) Интерфейс пользователя. С помощью него осуществляется диалог пользователя с программой.
2) Модуль формирования дерева каталогов. Формирует дерево всех папок и файлов, присутствующих на компьютере.
3) Модуль управления. Этот модуль ответственен за взаимодействие модулей между собой, их запуск.
4) Модуль установки параметров. Задаёт параметры для работы других модулей.
5) Модуль создания новых субъектов. Он ответственен за создание новых субъектов.

6) Модуль настройки субъектов. Настраивает свойства субъекта, такие как, например, присутствие его в определённой группе.
7) Модуль разграничения прав доступа. Изменяет права доступа субъектов к объектам – удаляет их или добавляет.
8) Модуль подсчёта фактов доступа. Обращается к журналу событий, собирает информацию о фактах доступа субъекта к объектам, подсчитывает их количество.

Интерфейс программного комплекса представлен ниже на Рисунке 3.

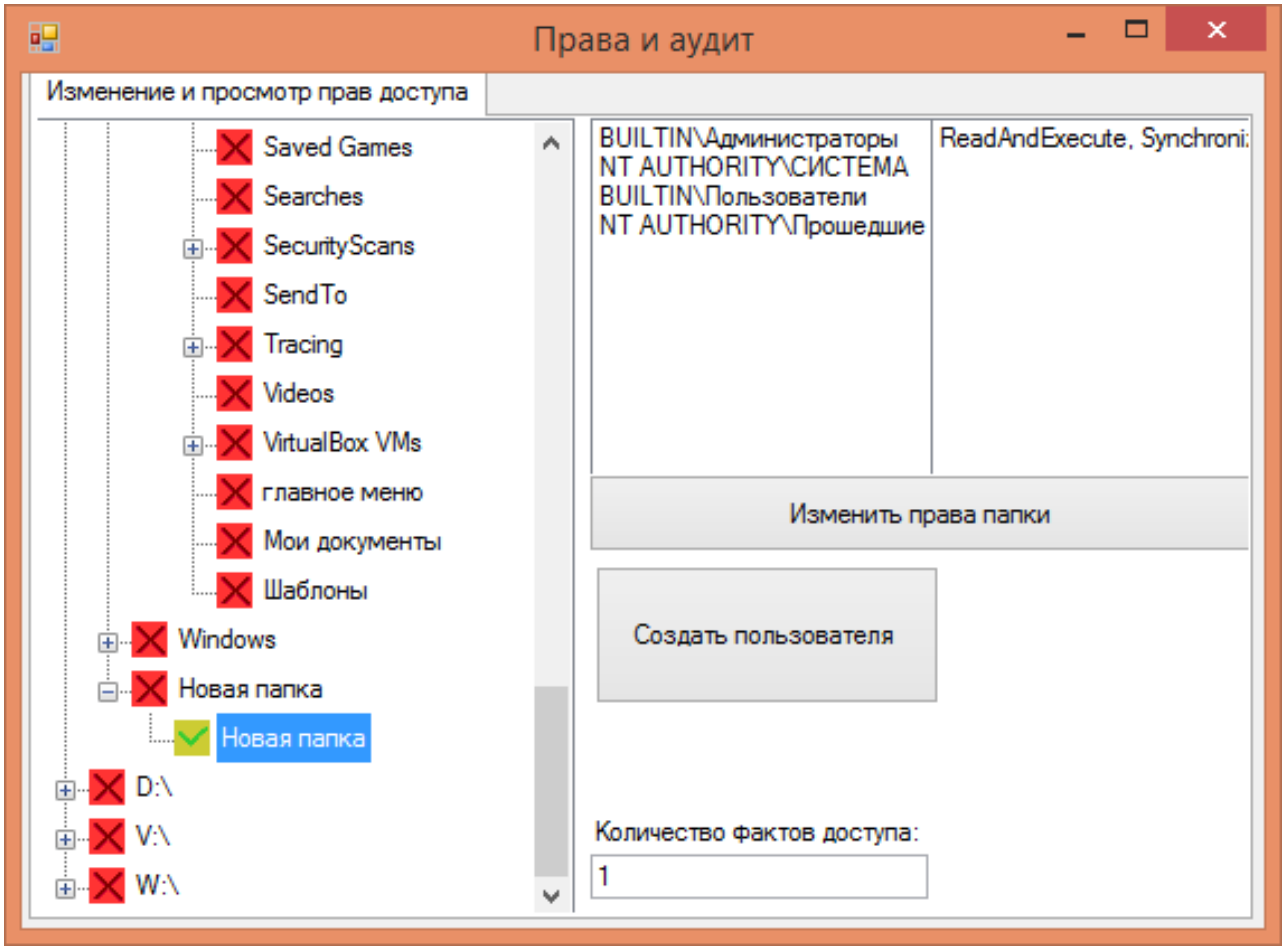

Рисунок 3 – Интерфейс программного комплекса

На Рисунке 3 выше слева находится дерево каталогов системы. Красным на нём обозначены те каталоги, к которым не осуществлялся доступ, зелёным – осуществлялся. При нажатии на каталог, отмеченным зелёным, возле дерева высвечивается количество фактов доступа к этому объекту. Также присутствуют блоки вывода список пользователей, имеющих доступ к объекту и их права доступа. Под ними находится кнопки изменения доступа субъектов к объектам и создания нового пользователя – последняя используется для создания пользователя посредника.

Заключение

Использование этого программного комплекса повысит эффективность работы администратора и позволит ему построить модель реального доступа к ресурсам, а также изолировать доступ к отдельным ресурсам.

Библиографический список

1. Антюфеев С. Ю. Гибридная объектная модель доступа к данным / С. Ю. Антюфеев, В. А. Астапчук, Е. Б. Гаврилов // Информационная безопасность. – 2005. – № 2. – С. 15–22.
2. Васильева М. И. Обеспечение безопасности данных ГИС Росводресурсов на основе дискреционной защиты / М. И. Васильева // Информатика, управление и компьютерные науки: актуальные проблемы в науке и технике : сб. ст. Третьей Всерос. зимней шк.-семинара аспирантов и молодых ученых, 20–23 февр. 2008 г. – Уфа : Диалог, 2008. – Т. 1. – С. 387–394.
3. Сборник руководящих документов по защите информации от несанкционированного доступа [Электронный ресурс] : инструкция : Утв. Приказом Гостехкомиссии РФ 1998. – Москва, 1998. – 85 с. – Режим доступа: http://www.zakonprost.ru/content/base/265902.
4. Лепешкин О. М. Подходы к обеспечению функциональной применимости ролевой модели разграничения доступа в системе управления предприятия / О. М. Лепешкин, П. В. Харечкин // Информационная безопасность : материалы IX Междунар. науч.-практ. конф. – Таганрог, 2007. – Ч. 1. – С. 235–241 ; Информационное противодействие угрозам терроризма. – 2008. – № 11. – С. 57–66.
5. Андрианов В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов ; под ред. А. П. Курило. – Москва : Альпина Паблишер, 2011. – 392 с.