Разработка моделей разграничения доступа автоматизированной информационной системы информационного центра МВД России

Жукова
Маргарита Александровна,
преподаватель кафедры информатики и математики Краснодарского университета МВД России,
старший лейтенант полиции

Информационной основой криминалистических, розыскных и оперативно-справочных учетов является сбор, накопление и анализ сведений о субъектах и предметах преступлений и связанных с ними событиях. Получение информации в этих учетах является важным процессуально следственным действием и осуществляется путем обращения в виде запросов в ИЦ, а при необходимости и в ГИЦ. Полученные данные используются в следственной, оперативно-розыскной и криминалистической деятельности правоохранительных органов как ориентирующий и диагностический материал, а также в целях идентификации. Вся выше перечисленная информация находится в автоматизированной информационной системе информационного центра (АИСИЦ).

Наличие в АИСИЦ различной конфиденциальной информации приводит к тому, что нарушение её доступности, целостности или конфиденциальности может привести к незаконному извлечению этой информации и повлечь причинение ущерба процессуально-следственным действиям. Все это требует необходимости организации защиты информации, циркулирующей в АИСИЦ.

Разработка систем защиты информации (СЗИ) требует моделирования этих систем, а также разработки механизма анализа эффективности функционирования СЗИ. Следовательно, разрабатываемые модели и механизмы анализа СЗИ должны проводиться с учетом перспективных направлений по обеспечению защищённости информации, в идеале позволяющих в процессе циркуляции информации не допускать уязвимостей.

Исследование показало, что противостояние угроз и средств защиты развиваются следующим образом: новые виды атак приводят к появлению новых средств защиты, а недостатки в средствах защиты приводят к появлению новых средств нападения и т.д.

Обеспечить гарантированную защиту информации АИСИЦ практически невозможно вследствие следующих факторов:

- Количество угроз постоянно увеличивается. Следовательно, для новых угроз будут необходимы новые меры защиты и т.д.
- Количество угроз постоянно увеличивается не только количественно, но и качественно.

В эталонной АИСИЦ доступ к информации реализуется путем последовательного спуска по уровням детализации ресурсов цепочкой авторизованных доступов компонентов более высокого уровня к ресурсам компонентов более низкого уровня.

Возможность структуризации процессов доступа к ресурсам в АИСИЦ имеет вполне естественную природу, которая заключена в иерархическом характере ресурсов. А именно, ресурсы АИСИЦ можно рассматривать с разным уровнем детализации. При рассмотрении каждого такого уровня необходимо абстрагирование от деталей реализации его компонентов, которые раскрываются на нижестоящих уровнях. В данном случае нижние 6 уровней не рассматриваются, так как на них происходят процессы преобразования информации, необходимые для её транспортировки по линиям связи, а нас интересуют процессы разграничения доступа (рис. 1).

Уровень 15 (*административный уровень*). Определяет доступ администратора к АИСИЦ. Администратор имеет широкие функциональные обязанности, в частности — предоставляет пользователям полномочия.

Уровень 14 (*идентификационный уровень*). Определяет доступ уполномоченного пользователя к АИСИЦ (процедуры идентификации и аутентификации). В результате устанавливается соответствие между уполномоченным пользователем и его идентификатором.

Уровень 13 (*интеграционный уровень*). Определяет доступ виртуального пользователя, авторизованного уполномоченным пользователем, к ресурсам АИСИЦ посредством создания интегрированной индивидуальной пользовательской рабочей среды интегратором АИСИЦ. Предполагается, что уполномоченный пользователь, прошедший процедуры идентификации и аутентификации, взаимодействует в определенной роли с АИСИЦ через интегратор, выполняющий функции интерфейса АИСИЦ с пользователем, при этом взаимодействие осуществляется, в общем случае, на удобном для пользователя языке.

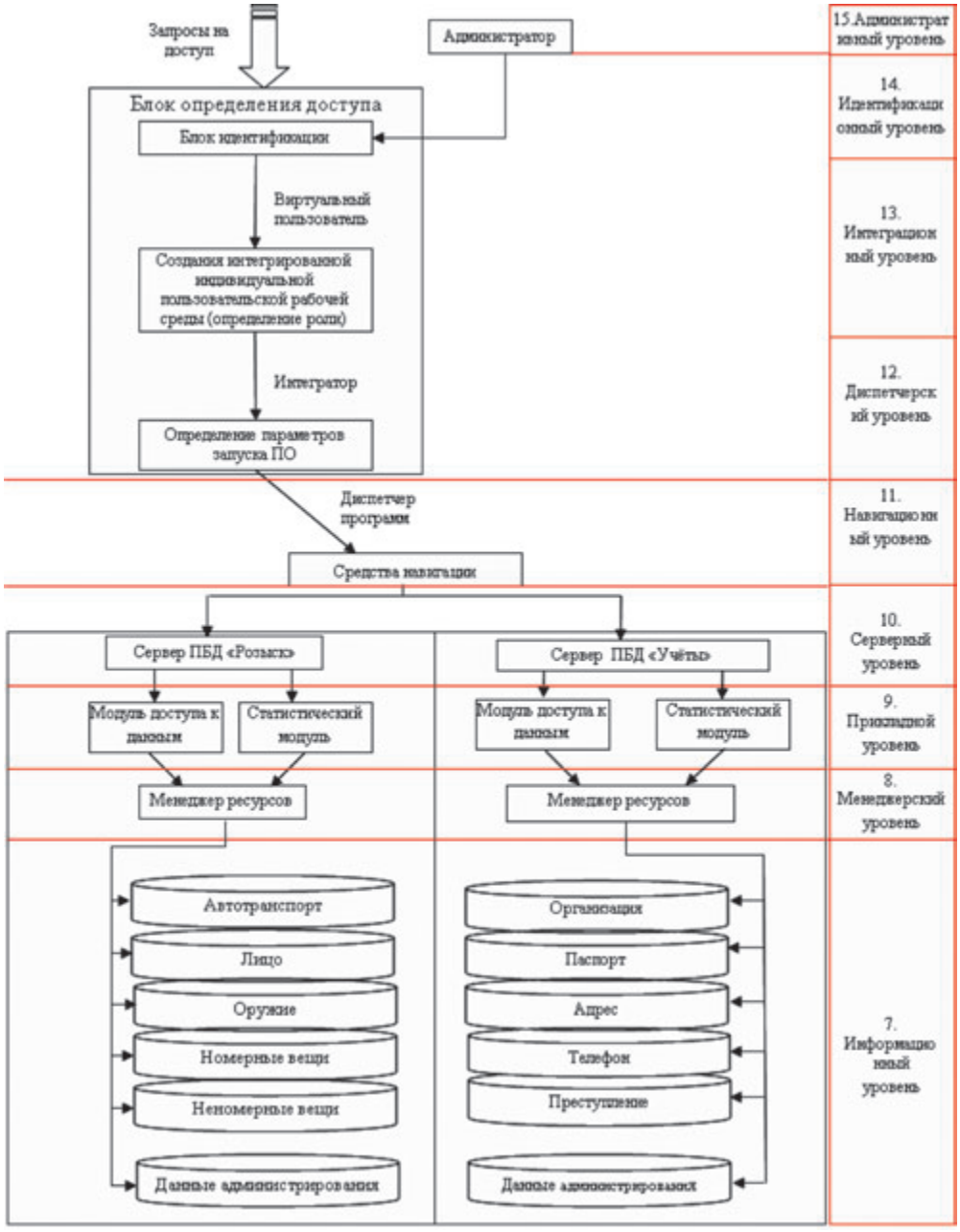

Рис. 1. Распределение элементов БД ИЦ по уровням ЭМЗАС

Уровень 12 (*диспетчерский уровень*). Определяет доступ интегратора АИСИЦ, авторизованного некоторым образом, к ресурсам АИСИЦ посредством управления запуском прикладных программ, осуществляемого диспетчером программ АИСИЦ.

Уровень 11 (*навигационный уровень*). Определяет доступ диспетчера программ, авторизованного некоторым образом, к средствам навигации АИСИЦ.

Уровень 10 (*серверный уровень*). Определяет доступ средства навигации АИСИЦ, авторизованного некоторым образом, к серверам АИСИЦ. В результате определенный сервер предоставляет свои услуги средству навигации в интересах пользователя, авторизующего доступ.

Уровень 9 (*прикладной уровень*). Определяет доступ сервера АИСИЦ, авторизованного некоторым образом, к подчиненным ему прикладным компонентам.

Уровень 8 (*менеджерский уровень*). Определяет доступ прикладного компонента сервера АИСИЦ, авторизованного некоторым образом, к менеджерам ресурсов данного сервера.

Уровень 7 (*информационный уровень*). Определяет доступ менеджера ресурсов сервера АИСИЦ, авторизованного некоторым образом, к данным, хранящимся на сервере. В результате определенные данные под управлением менеджера ресурсов используются в интересах пользователя, авторизующего доступ.