УДК 621.391

Способ построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации

А. В. Кузнецов
ООО «НТЦ «Вулкан», Москва, Россия

Рассмотрен способ построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации, основывающийся на анализе принципов предоставления прав доступа в автоматизированной информационной системе и реализации данной системы и ее окружения.

Ключевые слова: права доступа, системные привилегии, профиль внутренних нарушителей безопасности информации.

Проблема защиты информации в автоматизированных информационных системах (АИС) не теряет своей актуальности вот уже на протяжении ряда десятилетий. При ее решении одной из первостепенных задач является формирование модели нарушителя безопасности информации как неотъемлемой части процессов моделирования угроз, анализа рисков или оценки степени защищенности объектов защиты [1, 2]. Стоит отметить, что на сегодняшний день основную опасность представляют внутренние нарушители, т. е. лица, обладающие санкционированным правом доступа к защищаемой информации и/или технологическому окружению или обеспечению АИС, так как реализовать несанкционированный доступ к информации изнутри всегда гораздо проще, чем извне [3, 4]. Данный факт также подтверждается увеличением за последние годы количества утечек конфиденциальной информации [5].

Успешность и простота реализации угроз безопасности информации через существующие уязвимости АИС внутренним нарушителем зависит от предоставленных ему прав доступа и системных привилегий. Принимая во внимание данные сведения, необходимо выбирать наиболее подходящие защитные меры: превентивные, детективные, корректирующие, компенсирующие и/или сдерживающие.

Таким образом, для построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации необходимо определить:

- перечень объектов доступа с необходимым уровнем детализации;
- перечень субъектов доступа;
- права доступа субъектов доступа к объектам доступа (к данным);
- привилегии субъектов доступа в общесистемном и прикладном программном обеспечениях АИС.

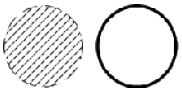
Сложность решения данной задачи обусловлена трудоемкой подготовительной работой и необходимостью учета различных параметров, связанных с данными (их представлением и группировкой), порядком их обработки и реализацией АИС, т. е. носит комплексный характер.

На сегодняшний день в зарубежной практике не принято разрабатывать отдельные модели нарушителей (Model of adversary/attacker) [6], но существуют рекомендации по формированию источников угроз безопасности информации (Threat source) [7, 8], которые носят более общий характер и в явном виде не затрагивают вопросы прав доступа и системных привилегий внутренних нарушителей безопасности информации. В российской нормативной базе для построения моделей нарушителей безопасности информации зачастую используются иерархические модели, т. е. каждый следующий уровень нарушителя безопасности информации включает в себя функциональные возможности предыдущего [9, 10]. Но данный подход обладает недостатком, так как права доступа и/или привилегии у различных типов нарушителей безопасности информации могут находиться в четырех вариациях, представленных на рис. 1 с использованием кругов Эйлера, и только одна из них является иерархической [11].

Кузнецов Александр Васильевич, руководитель отдела безопасности информационных систем.
Тел. 8 (495) 663-95-16. E-mail: a.kuznetsov@ntc-vulkan.ru

Статья поступила в редакцию 11 сентября 2013 г.

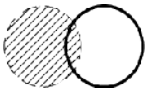
$Right_1 \in [1; R_1]$, $Right_2 \in [R_2; R]$



$Right_1 \cap Right_2 = 0$

Субъекты доступа не имеют общих прав/привилегий

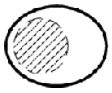
$Right_1 \in [1; R_1]$, $Right_2 \in [R_2; R]$



$Right_1 \cap Right_2 = [R_2; R_1]$

Субъекты доступа имеют ряд общих прав/привилегий

$Right_1 \in [1; R_1]$, $Right_2 \in [1; R_2]$



$Right_1 \cap Right_2 = [1; R_1]$,
$Right_1 \subset Right_2$

Права/привилегии одного субъекта доступа включены в права/привилегии другого

$Right_1 \in [1; R_1]$, $Right_2 \in [1; R_2]$

$Right_1 \cap Right_2 = [1; R_1] = [1; R_2]$,
$R_1 = R_2$

Права/привилегии субъектов доступа совпадают

Рис. 1. Варианты отношения прав доступа (системных привилегий) субъектов доступа

В ряде подходов [12—14] предлагается характеризовать нарушителя(ей) безопасности информации путем оценки мотивации и потенциала нападения (компетентность, доступные ресурсы, допустимый риск и т. п.). Для использования данных подходов необходимо иметь вероятностные или оценочные значения ряда величин, связанных с человеческим фактором, которые на практике получить крайне затруднительно, и, как следствие, невозможно получить не только объективную оценку, но и просто адекватный результат.

С учетом выше сказанного возникает потребность совершенствования существующих способов.

Цель данной статьи — разработка способа построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации, основанного на анализе принципов предоставления прав доступа в АИС и реализации данной системы и ее окружения, а также учитывающего недостатки иерархической модели и подходов, использующих оценку мотивации и потенциала нападения.

Первостепенно необходимо определить перечень объектов доступа с необходимым уровнем детализации. Уровень детализации ограничивается технической возможностью назначения прав доступа на "минимальный" объект доступа, т. е. реализацией АИС. Например:

1. Для файловых ресурсов — раздел/каталог/файл (содержимое/атрибуты);

2. Для баз данных — таблица/столбец/строка/запись/ячейка.

Преимуществом максимальной детализации перечня объектов доступа является строгая возможность разграничения прав доступа, а также прозрачность в рамках контроля. При этом недостатками являются повышенные затраты на поддержание данного перечня в актуальном состоянии.

На практике предлагается использовать итерационный подход, в рамках которого на первой стадии составления перечня объектов доступа могут использоваться высокоуровневые перечни, в которых объектом доступа выступают все данные, обрабатываемые в АИС. Дополнительно предлагается осуществлять формирование групп объектов доступа по категориям защищаемой информации (по уровню/категории конфиденциальности, критичности или т. п.).

Обобщенная блок-схема процесса формирования перечня объектов доступа представлена на рис. 2.

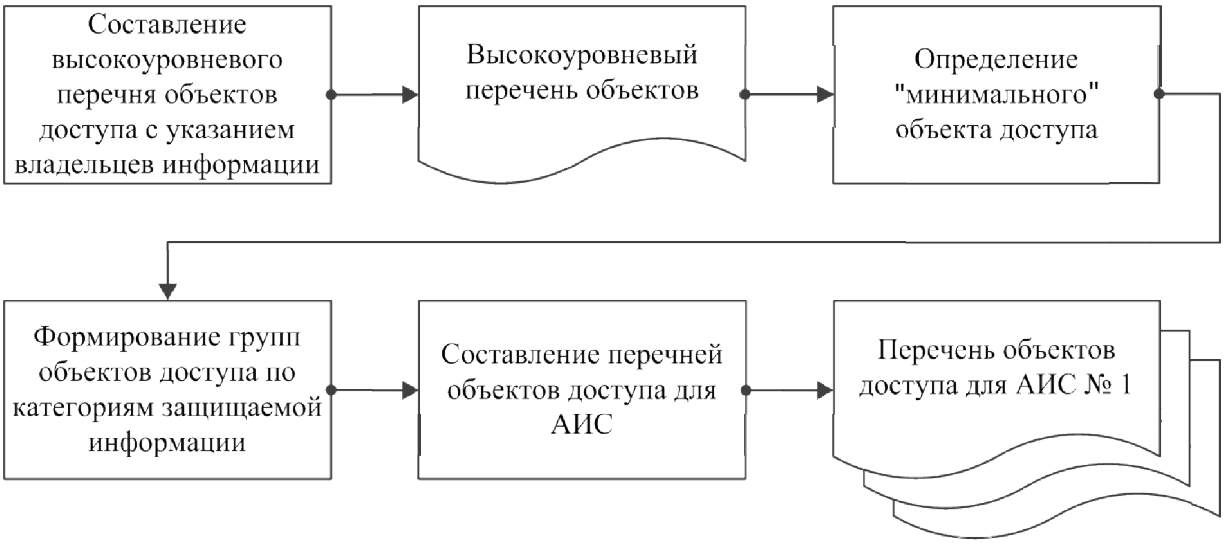


Рис. 2. Блок-схема процесса формирования перечня объектов доступа

Определение прав доступа к данным и системных привилегий должно проводиться для всех без исключения субъектов доступа — сотрудников организации, являющейся владельцем АИС, в том числе особо доверенных лиц, а также контрагентов (в случае наличия доступа к АИС). Определение данных значений проводится с максимально возможной долей достоверности, так как данные получаются из самих АИС и ее окружения, и не требует вероятностные или оценочные значения величин, связанных с человеческим фактором.

Перейдем к рассмотрению определения прав доступа субъектов доступа к объектам доступа. Здесь предлагается использовать следующие независимые значения прав доступа, т. е. ни одно из прав не зависит от наличия/отсутствия другого и/или не является вложенным:

- Нет доступа (No access);
- Чтение (Read);
- Запись (Write);
- Изменение, в том числе удаление (Change).

При этом не выделяется отдельно операция удаления, так как при наличии прав на изменение субъект доступа может провести обнуление содержимого объекта доступа (очистку или замену всех данными иными), не удаляя самого объекта. Таким образом, 100%-ая потеря целостности содержимого может быть по тяжести последствий приравнена к удалению самого объекта.

Стоит отметить, что данный подход инвариантен для основных принципов управления правами доступа: дискреционный и мандатный. В первом случае четыре указанные вида прав доступа могут быть использованы для составления всех возможных комбинаций (полным доступом считается комбинация: чтение + запись + изменение). Для мандатного принципа доступа устанавливается следующая комбинация указанных выше прав:

- для уровня доступа "L+1" — нет доступа;
- для уровня доступа "L" — чтение + запись + изменение;
- для уровня доступа "L–1" — чтение.

Таким образом, проанализировав принцип предоставления прав доступа в конкретной АИС, с использованием данных значений могут быть составлены необходимые комбинации прав доступа. При необходимости владельцами АИС данный перечень прав доступа может быть уточнен и/или скорректирован.

Перейдем к рассмотрению системных привилегий. Это важный момент, о котором очень часто забывают, при этом неподходящее использование системных привилегий (любая характеристика или средство АИС, которые дают пользователю возможность игнорировать средства управления системой или приложением) могут быть основным фактором, дающим вклад в сбои и/или нарушения в работе АИС [15].

Здесь предлагается использовать ролевые модели, реализуемые практически во всех видах общесистемного и прикладного программного обеспечения современных АИС, т. е. ориентироваться на реализацию конкретной АИС и ее окружения. Например:

- Администраторы (Administrators);
- Опытные пользователи (Power users);
- Пользователи (Users);
- Гости (Guests);
- Нет доступа (No access).

В случае использования для обработки данных (работы с объектом доступа) различного программного обеспечения рекомендуется выбирать наиболее привилегированное значение для данного субъекта доступа либо указывать все значения.

На заключительном этапе предлагается произвести наглядную визуализацию профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации:

- на оси абсцисс с равномерным шагом отметить точки для соответствующих прав доступа (четыре значения);
- на оси ординат с равномерным шагом отметить точки для соответствующих системных привилегий (рекомендуется расположить максимально и минимально привилегированные роли в противоположных концах на оси);
- на оси аппликат с равномерным шагом отметить точки для соответствующих объектов доступа;
- провести нанесений соответствующих значений в плоскостях *YZ* и *XZ* (рис. 3), при этом в плоскости XY никаких взаимосвязей нет;
- построить ортогональную проекцию значений в плоскостях *YZ* и *XZ* для использования на практике (рис. 4).

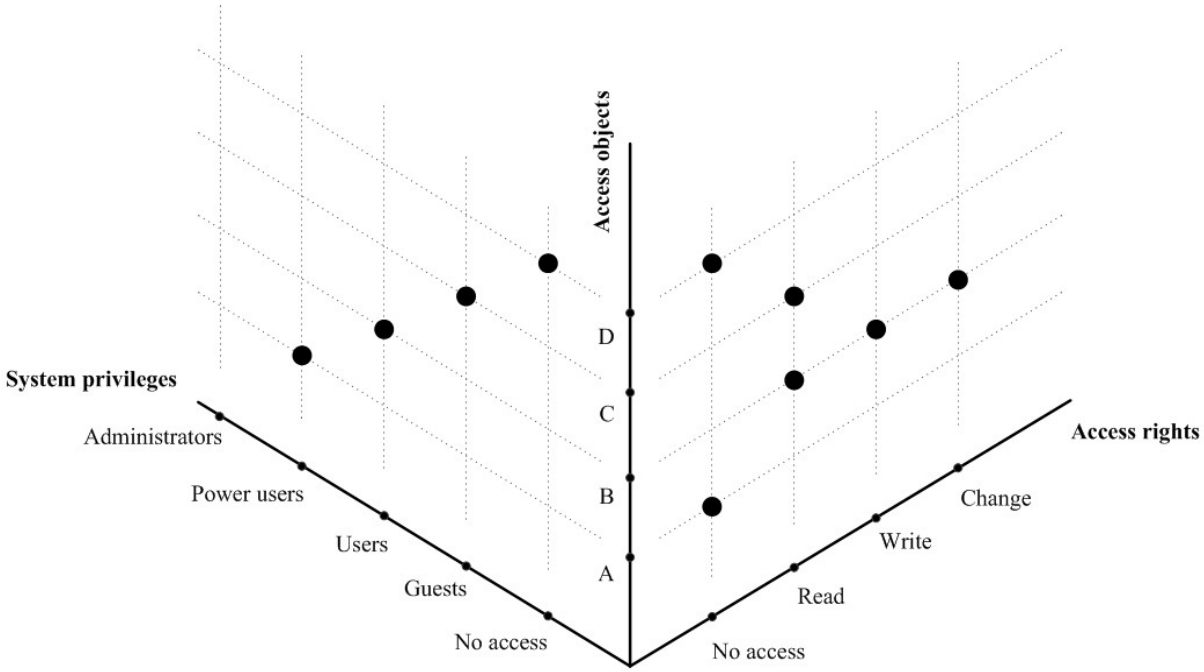


Рис. 3. Профиль прав доступа и системных привилегий

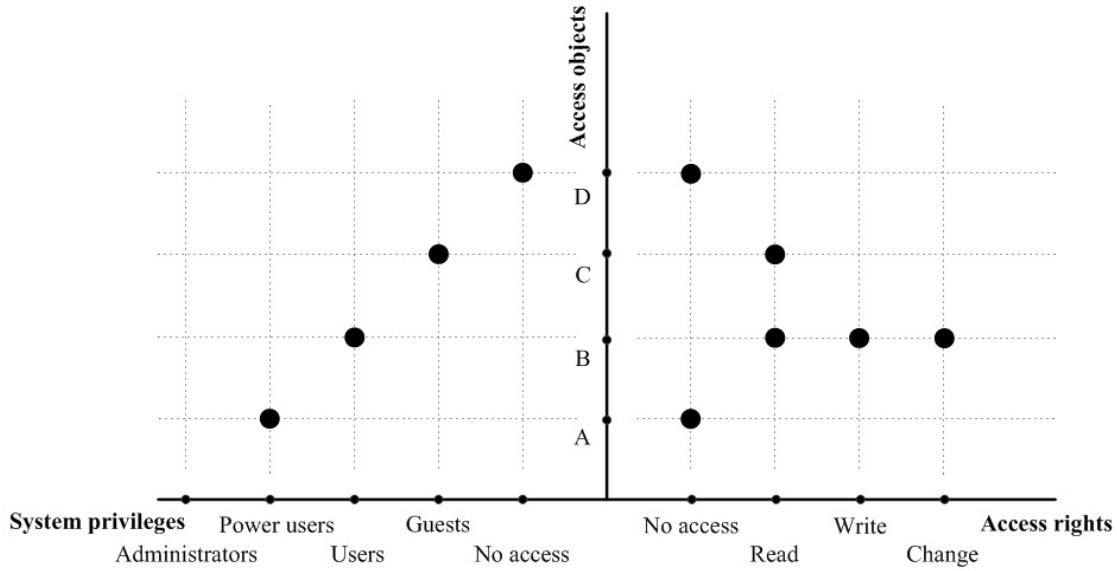


Рис. 4. Профиль прав доступа и системных привилегий (для использования на практике)

Данное представление является более наглядным, чем табличные матрицы доступа, так как если при чтении таблицы что-то остается незамеченным, то обнаруживается на графике [16]. Это позволяет, в том числе, оперативнее выявлять изменения прав/привилегий в случае использования автоматизированных средств построения данных профилей на базе информации, полученной от систем:

- управления идентификаторами и правами (Identity & Access/Rights Management);
- предотвращения утечек данных (Data Loss/Leak Prevention);
- управления событиями и информацией о безопасности (Security Information and Event Management).

Предлагаемый способ построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации представляет собой следующую последовательность действий:

1. Формирование высокоуровневого перечня объектов доступа с указанием владельцев.
2. Детализация владельцами объектов доступа.
3. Группировка объектов доступа по категориям защищаемой информации.
4. Формирование перечней объектов доступа.
5. Формирование перечня субъектов доступа.
6. Группировка субъектов доступа (в случае необходимости).
7. Определение прав доступа к данным.
8. Определение привилегий в общесистемном и прикладном программном обеспечениях АИС.
9. Построение профиля прав доступа и системных привилегий для каждого субъекта доступа (группы субъектов доступа).

Предложенный способ построения профилей прав доступа и системных привилегий внутренних нарушителей безопасности информации, основывающийся на анализе принципов предоставления прав доступа в АИС и реализации данной системы и ее окружения, носит комплексных характер и дополняет недостающую информацию для формирования моделей нарушителя безопасности информации. Полученные профили могут быть использованы в рамках процессов моделирования угроз, анализа рисков или оценки степени защищенности объектов защиты.

Предложенный способ в отличие от аналогов является инвариантным к реализации АИС и к используемым принципам предоставления прав доступа, что позволит, не меняя самого методического инструментария, применять его для различных объектов защиты, в том числе тех, которые появятся в результате развития информационных технологий.

Литература

1. *Кузнецов А. В.* Методика оценки степени защищенности информации в автоматизированных информационных системах / А. В. Кузнецов, А. А. Иржавский, А. Н. Захарченко // Наукоемкие технологии. 2011. № 8. Т. 12. С. 43–47.
2. *Кузнецов А. В.* Способ определения степени уязвимости автоматизированной информационной системы в отношении конкретных методов реализации угроз безопасности информации / А. В. Кузнецов, В. А. Михеев, М. М. Репин // Вопросы защиты информации. 2013. № 1 (100). С. 20—25.
3. *Кузнецов А. В.* Системы предотвращения утечки данных: первый шаг — он трудный самый [Электронный ресурс]: http://www.bytemag.ru/articles/detail.php?ID=16753. Проверено 01.09.2013.
4. *Андрианов В. В., Зефиров С. Л., Голованов В. Б.* Обеспечение информационной безопасности бизнеса. — 2-е изд. — М.: ЦИПСиРЖ Альпина Паблишерз, 2011. С. 220—234.
5. Утечки корпоративной информации и конфиденциальных данных за 2012 г. // Информационная безопасность. 2013. № 3. С. 8—11.
6. *Ken Jaworski*. Practice Course for Risk Management and Business Continuity Planning. April 2013.
7. NIST Special Publication 800-30. Revision 1 Guide for Conducting Risk Assessments. 2012, September. P. 17, 65—68.
8. *Ahmad Ali Al-Zubi*. Threats Sources Identification // Canadian Journal on Network and Information Security. V. 1. No. 1. April 2010. P. 38—43.
9. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России 1992-03-30. — 3 с.
10. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России № 149/54-144 2008-02-21.
11. *Кузнецов А. В.* // Тезисы доклада Способ определения уровня прав доступа групп пользователей в автоматизированных информационных системах. — Москва: XXV военно-научная конференция 18 ЦНИИ МО РФ, 2011.
12. *Шарамок А. В.* О методе разработки модели источника угроз // Вопросы защиты информации. 2013. № 1 (100). С. 26—31.
13. Мотиваторы и демотиваторы разных игроков рынка ИБ или почему регуляторам и потребителям сложно найти общий язык [Электронный ресурс]: http://lukatsky.blogspot.ru/2012/05/blog-post_04.html. Проверено 01.09.2013.
14. ГОСТ Р ИСО/МЭК 18045-2008. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Введен в действие 2009-09-30. — М.: Издательство стандартов, 2009. С. 218—223.
15. ISO ISO/IEC 27002. Информационные технологии. Свод правил по управлению защитой информации. Перевод на русский язык Компания "Технорматив". 2007. С. 94—95.
16. *Бурханова И. В.* Теория статистики: Конспект лекций. — М.: ЭКСМО, 2007. С. 37—38.

Method of developing access rights profiles and system privileges of internal adversaries

A. V. Kuznetcov
LLC "Research and Development Center "Vulkan", Moscow, Russia

In this article a method of building up access rights and system privileges profiles of internal adversaries is described. The technique is based on the analysis of various methods of providing the access control in an automated information system and the implementation of one and its environment.

Keywords: access rights, system privileges, profiles of internal adversaries.

Bibliography — 16 references. *Received September 11, 2013*