Управление доступом в системах электронного документооборота

А. Ю. Даниленко

Институт системного анализа Российской академии наук,
Россия, 117312 Москва, пр. 60-летия Октября, 9

На примере программного комплекса «Евфрат-Документооборот» рассмотрены основные принципы и особенности реализации подсистемы управления доступом для защищенных информационных систем.

Введение

В работах [1–5] рассмотрены основные особенности проектирования и разработки сложных информационных систем. Обосновывается также необходимость реализации в них средств защиты информации, которые должны обеспечить возможность работы этих систем с конфиденциальной информацией, в частности с персональными данными. Одним из средств защиты информации для автоматизированных систем группы «1» по классификации ФСТЭК[1] [6] является подсистема управления доступом.

Одним из распространенных классов информационных систем являются системы электронного документооборота (СЭДО), характерными особенностями которых являются большое число пользователей системы, большое число информационных объектов, а также сложность этих объектов и невозможность работать с ними исключительно с помощью средств, предоставляемых СУБД. Рассматриваемые далее особенности систем и подходы к их разработке применимы к любым системам электронного документооборота, однако для простоты мы, в качестве примера, будем иметь в виду программный комплекс «Евфрат-Документооборот».

[1] ФСТЭК — Федеральная служба по техническому и экспортному контролю, один из органов, уполномо-ченных заниматься проблемами защиты информации в РФ, правоприемник Гостехкомиссии.

1. Объектная модель данных СЭДО

Из всего множества информационных объектов, которыми оперирует типичная СЭДО, нас будут интересовать данные о пользователях и их свойствах, а также те объекты, с которыми пользователи непосредственно работают.

1.1. Данные пользователей

1. Общая информация о пользователях:
   – отображаемое имя;
   – должность, телефон, подразделение и другие подобные свойства.
2. Информация, используемая при работе подсистемы управления доступом:
   – внутренний системный идентификатор;
   – системное имя для входа в систему (логин);
   – пароль для входа в систему;
   – членство в группах, соответствующих организационной структуре предприятия;
   – членство в системных группах СЭДО (списки рассылки, группы доступа и т. п.);
   – привилегии, например администраторы СЭДО.

1.2. Объекты, с которыми работают пользователи

1. Электронные документы:
   – структура документа;
   – значения реквизитов для поиска;
   – файлы с содержательной информацией (присоединенные файлы);
   – списки управления доступом (аналогично Access control list, описывающим правила доступа к объектам операционной системы).
2. Поручения:
   – текст поручения;
   – срок исполнения поручения;
   – ход исполнения;
   – исполнители поручения;
   – контролер.
3. Письма внутренней почтовой системы:
   – отправитель письма;
   – адресаты письма;

– тема письма;
– текст письма;
– идентификатор документа, присоединенного к письму (аналогично файлам для случая обычных почтовых систем).

4. Автоматически создаваемые уведомления системы управления потоками работ о назначении исполнителями и контролерами поручений, о приближении сроков исполнения и т. д.

2. Построение модели безопасности СЭДО

Как известно [3], модель безопасности для информационной системы состоит из следующих основных разделов:

- Модель нарушителя, в которой дается описание предполагаемого нарушителя, стоящих перед ним задач и уровень его возможностей (включая квалификацию).
- Модель угроз, в которой описываются как угрозы, направленные на несанкционированный доступ к информации, так и угрозы, связанные с возможностью утраты хранимых данных, — аварии, пожары, землетрясения и т. д.
- Субъекты защиты — лица, от неправомерных действий которых предусматривается защита данных. Нас в этой части будут интересовать только легальные пользователи системы, т. е. пользователи, зарегистрированные в системе, имеющие право работать в ней, обладающие некоторым набором полномочий и прав по отношению к информационным объектам, которыми оперирует СЭДО.
- Объекты защиты — те информационные объекты, которые должны быть защищены от несанкционированного доступа. Отметим, что для различных информационных объектов системы подход к защите может принципиально отличаться. Например, открытые ключи для проверки электронно-цифровой подписи (ЭЦП) (или сертификаты открытого ключа) должны быть доступны для чтения всем пользователям системы (при этом модификация этих объектов запрещена, возможно только уничтожение и создание новых), электронные документы должны быть доступны ограниченному кругу пользователей, письма — только адресатам, а протоколы событий, происходящих в системе, — административному персоналу.
- Перечень действий, возможных с объектами. Для большинства объектов это создание, чтение его (просмотр), редактирование, уничтожение. Для электронных документов вводится дополнительное действие — изменение прав доступа. В зависимости от назначения системы воз-

можно более детальное рассмотрение действий, например в некоторых случаях отдельно выделяют право на присоединение к документу файлов.

- Правила определения допустимости действий субъектов над объектами, исходя из полномочий субъектов в системе и атрибутов безопасности объектов. Во многих случаях выдвигается требование работы по разным правилам с различными частями информационного объекта. Например доступ к присоединенным файлам документа может контролироваться более жестко, чем доступ к регистрационной карточке.

3. Пример реализации системы управления доступом

При проектировании информационных систем, сходных по сложности с СЭДО, надо четко различать действия и ограничения, обусловленные деловой логикой и требованиями безопасности. В этой части, помимо очевидного утверждения о приоритетности требований безопасности по сравнению с деловой логикой, существует несколько моментов, часто вызывающих непонимание. Так, логика работы системы безопасности должна обеспечивать надежную защиту данных от несанкционированного доступа и в то же время должна быть максимально проста для проверки в ходе сертификационных исследований. Алгоритмы работы системы, реализующие деловую логику, призваны обеспечить точное выполнение делопроизводственных операций, что может и не совпадать с требованиями по защите информации.

Приведем два примера. В случае отправки пользователем письма через внутреннюю почтовую систему с точки зрения безопасности не существует ограничений на выбор адресатов этого сообщения, поскольку именно создатель объекта определяет, кому предназначена пересылаемая информация. Однако с точки зрения организации работы на предприятии возможно введение ограничений на это действие, например письмо директору могут направить только руководители не ниже некоторого уровня иерархии, а рядовые сотрудники могут адресовать свои письма только сотрудникам своего подразделения.

При работе с документом нескольких сотрудников этот процесс может быть организован как последовательный, при котором каждый из исполнителей документа начинает свою работу после завершения работы его предшественника. Однако руководитель, давая задание этой группе исполнителей, уже дал право на редактирование документа всем им. Здесь налицо различие алгоритма работы системы безопасности (доступ к документу предоставлен всем) и деловой логики (доступ к документу предоставляется последовательно по мере завершения предыдущего этапа работы).

Следующей особенностью работы таких систем является уже отмеченная сложность структуры информационных объектов. Каждый из них представлен в базе данных большим числом записей в разных таблицах (в случае иерархической базы данных в разных поддеревьях), а также различными файлами. Это приводит к тому, что использовать штатные средства разграничения доступа, входящие в СУБД, становится невозможным, поскольку они работают на уровне таблиц и колонок. В связи с этим сервер программного комплекса обращается к базе данных под одной привилегированной учетной записью, имеющей полный доступ к любым объектам СУБД и хранимым файлам, а разграничение доступа делается на уровне самого сервера, выполняющего чтение атрибутов безопасности (свойства как информационных объектов, так и пользователей) из базы данных и определение доступности тех или иных действий.

Рассмотрим (см. табл. 1) в качестве примера правила разграничения доступа к информационным объектам, реализованные в комплексе «Евфрат-Документооборот» (следует иметь в виду, что в этой системе для документов и поручений право на модификацию означает право на чтение).

Таблица 1

Объект	Создание	Чтение	Модификация	Уничтожение	Изменение прав доступа
Документ	Любой пользователь системы	Исполнители поручения по документу	Создатель, администратор, ответственный исполнитель и контролер поручения по документу	Администратор	Пользователи, имеющие право редактировать документ
Письмо	Любой пользователь системы	Адресат письма	Не предусмотрена	Автоматически после прочтения	Не предусмотрено
Поручение	Пользователи, имеющие право редактировать документ	Пользователи, имеющие право читать документ	Пользователи, имеющие право редактировать документ	Отдельно уничтожение поручений не предусмотрено, уничтожаются вместе с документом	Отдельно изменение прав для поручений не предусмотрено, они меняются вместе с правами на документ

Окончание таблицы 1

Объект	Создание	Чтение	Модификация	Уничтожение	Изменение прав доступа
Протоколы работы	Создается автоматически при установке системы	Администратор	Дописывает любой пользователь (точнее, сама система от имени пользователей)	Администратор	Не предусмотрено
Закрытые ключи ЭЦП	Администратор (в некоторых реализациях сами пользователи)	Владелец ключа	Не предусмотрена	Администратор	Не предусмотрено
Открытые ключи ЭЦП	Администратор (в некоторых реализациях сами пользователи)	Любой пользователь системы	Не предусмотрена	Администратор	Не предусмотрено

Литература

1. *Баранов А. П.* Проблемы создания и развития отечественных защищенных операционных систем // Методы и технические средства обеспечения безопасности информации: Материалы XVII Общероссийской научно-технической конференции. СПб.: Изд-во Политехнического университета, 2008. С. 76–78.
2. *Даниленко А. Ю.* Защита данных в сложных информационных системах // Обработка изображений и анализ данных: Сб. трудов ИСА РАН / Под ред. чл.-корр. РАН В. Л. Арлазарова и д. т. н. проф. Н. Е. Емельянова. М.: Книжный дом «Либроком»/URSS, 2008. С. 45–53.
3. *Даниленко А. Ю.* Обеспечение безопасного функционирования больших информационных систем // Информационно-аналитические аспекты в задачах управления: Сб. трудов ИСА РАН / Под ред. чл.-корр. РАН В. Л. Арлазарова и д. т. н. проф. Н. Е. Емельянова. М,: Издательство ЛКИ/URSS, 2007. С. 49–58.
4. *Вихорев С., Кобцев Р.* Как определить источники угроз // Открытые системы. 2002. № 7–8.
5. *Галатенко В.* Информационная безопасность // Открытые системы. 1995. № 4–6.
6. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.

7. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. М., 2002.
8. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. М., 1992.
9. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.
10. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. М., 1992.
11. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.