Оценка времени работы алгоритма Дейкстры в зависимости от числа вершин исходного графа будет $O(N^2)$ [6], где N — число вершин. Для построения графа G'_0 потребуется также $O(N^2)$ операций.

Для произвольного графа доступов необходимо найти *острова* в нем, а также *мосты*, их *начальный* и *конечный пролеты* [2–4]. Для поиска островов воспользуемся алгоритмом Флойда для поиска всех кратчайших путей [5].

Построим граф G_0^* по исходному графу доступов G_0 следующим образом:

1) множество вершин графа G_0^* совпадает с множеством вершин графа G_0 ($V_0^* = V_0$);
2) ребра в графе G_0^* не ориентированы; множество ребер графа включает лишь те ребра из G_0, для которых началом и концом дуги является вершина-субъект и которые содержат права *Take* или *Grant* ($E_0^* = E_0 \setminus (E_0^{s-o} \cup E_0^{\alpha})$, где E_0^{s-o} — множество ребер графа G_0, для которых начало и конец не являются субъектами; E_0^{α} — множество ребер графа G_0, не содержащих прав *Take* или *Grant*);
3) все ребра графа G_0^* имеют одинаковый вес.

Для графа G_0^* применим алгоритм Флойда. Алгоритм обнаружит кратчайшие пути между каждой парой вершин в графе G_0^*. Кратчайшие пути в графе G_0^* будут tg-путями, проходящими через вершины-субъекты в графе G_0. А сами вершины-субъекты, объединенные tg-путями, будут являться островами в графе G_0. Трудоемкость алгоритма Флойда — $O(N^3)$ [6]; граф G_0^* можно будет построить за $O(N^2)$ операций.

Зная критерии безопасности состояний информационной системы и способы проверки этих критериев, можно проанализировать исходное состояние системы на предмет наличия нежелательных доступов.

ЛИТЕРАТУРА

1. DoD 5200.28 – std. Department of Defense Trusted Computer System Evaluation Criteria. 1985.
2. *Lipton, Richard J.* A Linear Time Algorithm for Deciding Subject Security // J. ACM (Addison-Wesley). 1977. No. 3. P. 455–464.
3. *Девянин П. Н.* Модели безопасности компьютерных систем: учебное пособие для студентов высших учебных заведений. М.: Академия, 2005. 144 с.
4. *Гайдамакин Н. А.* Разграничения доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
5. *Майника Э.* Алгоритмы оптимизации на сетях и графах. М.: Мир, 1981. 324 с.
6. *Кормен Т., Лейзерсон Ч.* Алгоритмы: построение и анализ М.: МЦНМО, 2000. 960 с.

УДК 004.94

МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В ЭЛЕКТРОННЫХ ПОЧТОВЫХ СИСТЕМАХ[1]

К. А. Грищенко

В результате проведенного исследования распространенных электронных почтовых систем (ЭПС) получено описание реализованных в них механизмов управления

[1]Работа выполнена при поддержке гранта МД № 2.2010.10.

доступом и информационными потоками. Как правило, в состав ЭПС входят серверные и клиентские компоненты; в них производится хранение и обработка данных, организованных в виде набора документов. Документы хранятся в специальных базах данных, являющихся файлами ОС, в среде которой функционирует ЭПС. При этом возможно создание дополнительного программного обеспечения (ПО), использующего механизмы ЭПС для доступа к хранящимся в ЭПС данным.

Средствами ЭПС возможна организация разграничения доступа пользователей к обрабатываемым данным на различных уровнях — доступа клиентов к серверу, доступа пользователей к базам данных, доступа к отдельным полям документов. Разграничение доступа в ЭПС, как правило, является дискреционным.

Таким образом, для обеспечения возможности теоретического анализа безопасности ЭПС целесообразно построить ее формальную модель (ЭПС ДП-модель), взяв за основу ФАС и ФПАС ДП-модели [1, 2], позволяющие анализировать КС с дискреционным управлением доступом с функционально и параметрически ассоциированными сущностями. Кроме того, целесообразно учесть результаты, полученные при построении ФС ДП-модели [3], которая предназначена для исследования механизмов файловых систем, реализующих функции кодирования (например, криптографической защиты) данных.

При этом для построения ЭПС ДП-модели в ФАС, ФПАС и ФС ДП-модели предполагается внести изменения, позволяющие учитывать существенные особенности архитектуры ЭПС и реализации в ней механизмов разграничения доступа. Так, например, необходимо учесть клиент-серверную архитектуру ЭПС.

В современных ЭПС минимальной единицей обрабатываемых данных, доступ к которым разграничивается средствами самой ЭПС, может являться поле, входящее в состав документа, являющегося частью базы данных документов. Таким образом, в рамках ЭПС ДП-модели будем рассматривать сущности-поля, подчиненные в иерархии сущностям-документам, которые подчинены сущностям-базам данных.

Многие современные ЭПС предоставляют пользователям возможность совместной работы с документами. При этом разграничение доступа пользователей к таким документам часто осуществляется с использованием средств кодирования существенных частей документов. Пользователь может получить доступ ко всему документу, только обладая необходимыми данными (например, ключом).

Таким образом, при описании ЭПС ДП-модели используется следующее предположение.

Предположение. В рамках ЭПС ДП-модели выполняются следующие условия.

Условие 1. Система состоит из одного компьютера-сервера и нескольких (минимум одного) компьютеров-клиентов, на которых функционируют субъекты-операционные системы, реализующие среду для выполнения ПО сервера и клиентов. На компьютере-сервере субъекту-операционной системе подчинен в иерархии доверенный субъект-сервер, которому подчинены в иерархии доверенные субъекты-задачи. Субъекту-задаче в ЭПС ДП-модели соответствуют процессы в ОС (или их потоки), реализующие механизмы доступа клиентов к серверу, маршрутизации почты, репликации баз данных и др.

Условие 2. На компьютере-клиенте функционирует субъект-клиент, иерархически подчиненный субъекту-операционной системе компьютера-клиента.

Условие 3. В множестве сущностей выделено подмножество сущностей, защищенных ЭПС и не являющихся субъектами. В множестве доверенных субъектов-задач выделено подмножество субъектов, обладающих правами доступа и реализующих до-

ступ к сущностям, защищенным ЭПС, и кодирование в них данных в случае, когда оно осуществляется ЭПС. Эти доверенные субъекты реализуют информационные потоки по памяти между каждой сущностью, защищенной ЭПС, и соответствующей ей сущностью-образом, не являющейся субъектом.

Условие 4. Доверенные или недоверенные субъекты, не реализующие доступ к сущностям, защищенным ЭПС, не обладают правами доступа и не могут получать доступ к этим сущностям. При этом они могут обладать правами доступа или получать доступ к сущностям-образам сущностей, защищенных ЭПС.

Условие 5. Недоверенный субъект-задача может создать доверенного субъекта в случае, когда недоверенный субъект реализовал к себе информационные потоки по памяти от всех сущностей, параметрически ассоциированных с некоторым потенциальным доверенным субъектом.

При анализе безопасности ЭПС представляют интерес вопросы, связанные с возможностью получения нарушителем доступа к документам в обход правил политики безопасности. Для разрабатываемой ЭПС ДП-модели строятся формальные описания моделей нарушителя различных видов, а именно:

— нарушителя, являющегося зарегистрированным пользователем ЭПС;
— нарушителя, не являющегося зарегистрированным пользователем ЭПС, но имеющего возможность запускать процессы в ОС сервера ЭПС;
— нарушителя, не являющегося зарегистрированным пользователем ЭПС, но имеющего возможность прослушивать каналы связи между клиентами и сервером ЭПС и выступать в роли клиента ЭПС.

На основе ЭПС ДП-модели с использованием данных моделей нарушителя производится анализ возможности получения недоверенными субъектами доступа к сущностям, защищенным ЭПС, а также реализации от данных сущностей запрещенных информационных потоков. В результате предполагается разработать рекомендации по проектированию защищенных ЭПС.

ЛИТЕРАТУРА

1. *Девянин П Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
2. *Колегов Д Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнева. 2009. Вып. 1(22). Ч. 1. С. 49–54.
3. *Буренин П В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. № 1(3). С. 93–112.

УДК 004.94

РЕЗУЛЬТАТЫ АНАЛИЗА БЕЗОПАСНОСТИ СИСТЕМ С ПРОСТЫМИ ТРАЕКТОРИЯМИ ФУНКЦИОНИРОВАНИЯ В РАМКАХ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ[1]

П. Н. Девянин

На основе базовой ролевой ДП-модели (БР ДП-модели) [1, 2] рассматриваются условия передачи прав доступа и реализации информационных потоков по памяти для случая, когда на траекториях функционирования системы субъект-сессии не получают

[1]Работа выполнена при поддержке гранта МД № 2.2010.10.