СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕТИПОВЫХ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Захаров Александр Анатольевич
Д.т.н., профессор, Тюменский государственный университет
Варнавский Владислав Валерьевич
Аспирант, Тюменский государственный университет
vvv_90_08@mail.ru

Аннотация. В статье приводится подробный анализ моделей разграничения доступа для информационных систем узкого назначения. В начале статьи автор описывает преимущества и недостатки дискреционной и мандатной моделей доступа, делает вывод о крайне малой эффективности использования стандартных моделей доступа в информационных системах узкого назначения. Формирует критерии для сравнительного анализа нетиповых моделей доступа. В основной части статьи автор рассматривает модели разграничения доступа в контексте сформулированных критериев. В конце статьи автор делает обобщающий вывод по сравнительному анализу.

Ключевые слова: информационная безопасность; разграничение доступа; авторизация; модели разграничения доступа; контроль доступа.

COMPARATIVE ANALYSIS OF NON-STANDARD MODELS OF ACCESS CONTROL IN INFORMATION SYSTEMS

A. Zakharov
V. Varnavsky

Summary. The article provides a detailed analysis of access control models for information systems of narrow purpose. At the beginning of the article the author describes the advantages and disadvantages of discretionary and mandatory models for access, making the conclusion about the extremely low efficiency in the use of standard models in the information systems of narrow purpose. Forms criteria for comparative analysis of non-typical access models. In the main part of the article the author considers the models of access control in the context of the formulated criteria. At the end of the article the author makes a generalizing conclusion on comparative analysis.

Keywords: information security; access control; authorization; models of access control.

С развитием информационных технологий возникла проблема, при которой несколько пользователей должны работать в рамках одной информационной системы (ИС) одновременно. Современные ИС обеспечивают одновременную работу десятков тысяч пользователей. Для определения прав и привилегий пользователей используются модели разграничения доступа, основанные, как правило, на избирательной или полномочной политике доступа.

Большинство существующих моделей доступа ориентированы на предотвращение угроз, направленных на одно из основных свойств информации с точки зрения безопасности — конфиденциальности, целостности и доступности.

Наиболее часто используемыми моделями разграничения доступа в ИС являются модель избирательного управления доступом (далее — дискреционная модель),

которая нашла применение в семействе ОС Windows, и классическая модель мандатного управления доступом (далее — мандатная модель), используемая, например, в военных информационных системах, где наличие грифов секретности информации обуславливается требованиями законодательства.

Каждая модель является неотъемлемой частью системы контроля, управления и разграничения доступа информационных систем (далее — СКУД) и имеет свои преимущества и недостатки. Говоря о дискреционной модели, можно выделить следующие преимущества:

- простота реализации (данная модель основывается на проверке наличия явно указанных прав в матрице доступа или списках контроля доступа);
- гибкость настройки (для каждого субъекта возможно явно указать права на каждый объект).

Однако имеется и ряд недостатков:

- отсутствие механизмов контроля конфиденциальной информации (не предусмотрены механизмы ограничения передачи прав между субъектами);
- возможность получения неограниченного доступа администраторами системы;
- сложность в администрировании (для более точной настройки необходимо вручную назначать права доступа всем субъектам);
- хранение избыточной информации (в случае использования матриц доступа, связка «субъект»-«объект» имеется для всех пар участников отношений вне зависимости от реального положения дел), что может привести к утечке прав доступа [1].

К преимуществам мандатной модели можно отнести:

- простота администрирования (достаточно присваивать субъектам и объектам метки безопасности, не указывая явных прав);
- управление процессом разграничения доступа системой, а не пользователями (владелец не имеет полного доступа к своим ресурсам);
- отсутствие «суперпользователя»;
- контроль за потоками информации.

Недостатками являются:

- избыточность прав доступа (пользователи имеют равные права в пределах одного уровня безопасности);
- отсутствие гибкости в настройки (невозможно назначить особый уровень привилегий конкретному пользователю) [2].

Говоря о системах общего назначения, не предъявляющих сложных требований к разграничению доступа, следует отметить, что использование стандартной дискреционной или мандатной модели является оправданным по причине простоты их реализации и достаточности функционала. Примерами таких систем могут являться операционные системы, предназначенные для домашних пользователей, или системы управления базами данных в случае обработки не конфиденциальной информации.

Однако информационные системы специального назначения (например, военные, медицинские, ИСПДн и т.д.) предъявляют ряд дополнительных требований к разграничению доступа. Например, доступ к данным в медицинских информационных системах должен динамически изменяться в зависимости от:

- времени доступа к данным;
- текущих взаимоотношений врач;
- статуса пациента;
- места пребывания пациента;
- степени конфиденциальности информации [3].

Исходя из вышесказанного следует вывод, что использование стандартных моделей неэффективно с точки зрения безопасности в информационных системах специального назначения, для которых приведенные недостатки могут стать причиной фатальных ошибок.

Таким образом, актуальной проблемой является анализ существующих нетиповых моделей доступа и выявление наиболее эффективных с точки зрения обеспечения информационной безопасности.

В качестве критериев для анализа предлагаются:

- простота реализации (неверное выполнение шагов на этапе проектирования ИС может привести к инцидентам в области информационной безопасности);
- простота администрирования (для наибольшей эффективности СКУД необходимо нивелировать человеческий фактор);
- избыточность прав доступа;
- гибкость настройки;
- контроль защиты конфиденциальности информации;
- контроль защиты целостности информации;
- контроль защиты доступности информации;

Модель невмешательства

Модель невмешательства основана на мандатной политике разграничения доступа и направлена на решение проблемы утечки информации по скрытым каналам (ситуации, при которых информационные потоки протекают в обход стандартных правил «Нет чтения вверх» и «Нет записи вниз»). Вводится понятие «невмешатель-

ство» — т.е. ограничение, при котором ввод высоко уровневого пользователя не может смешиваться с выводом низкоуровневого пользователя.

В системе рассматриваются четыре объекта:
- высокий ввод (*high-in*);
- высокий вывод (*high-out*);
- низкий ввод (*low-in*);
- низкий вывод (*low-out*).

Данная модель включает использование следующих объектов и функций:
- *command(u)* — команда, исполненная пользователем u;
- *hist.command(u)* — история ввода системы, чей последний ввод был *command(u);*
- *out(u, hist.command(u))* — вывод пользователю u при исполнении команды *command*;
- *purge(u, hist)* — функция очищения команд, введенных пользователем;
- *clearence(u)* — функция определения степень доверия к пользователю.

Система считается удовлетворяющей требованию невмешательства, если для всех пользователей u, всех историй hist и всех команд вывода command справедливо:

out(u, hist.command(u))=out(u, purge(u, hist). command(u)) [4]

При сравнении данной модели с моделью Белла-Лападулы, являющейся классическим представителем моделей мандатного разграничения доступа, выделяют следующее:
- модель невмешательства контролирует процесс утечки информации по скрытым каналам за счёт введения концепции невмешательства;
- модель невмешательства, однако, позволяет копировать низкоуровневым пользователям один высокоуровневый файл в другой, что невозможно в модели БеллаЛападулы.

Как и модель Белла-Лападулы, модель невмешательства решает проблему защиты только одного свойства информации — конфиденциальности. Несмотря на наличие защиты от утечек по скрытым каналам, данная модель является менее гибкой, по причине наличия только двух категорий объектов, а также является сложной в реализации. При этом проблема наличия избыточных прав не решается.

Модель невыводимости

Наряду с моделью невмешательства данная модель направлена на решение проблемы утечки информации по скрытым каналам. Вводится понятия «Невыводимо безопасной» системы. Система является таковой, если пользователи с низкими уровнями безопасности не могут получить информацию с высоким уровнем безопасности в результате любых действий пользователей с высоким уровнем безопасности, т.е. утечка информации не может произойти в результате посылки высокоуровневыми пользователями высокоуровневой информации к низкоуровневым пользователям [5].

При использовании данной модели система принимает ввод от высоко– и низкоуровневых пользователей, обрабатывает эти вводы некоторым незаданным образом и затем выдает на выходах к высоко– и низкоуровневым пользователям информацию. Возможно также, что вводят информацию и получают данные вывода одни и те же пользователи. Единственным различием пользователей является то, какой у них уровень безопасности — высокий или низкий.

Данная модель является негибкой, по причине наличие только двух уровней безопасности пользователей, а также процесс ее реализации является крайне тяжелым, т.к. полностью изолировать пользователей различных групп, оставив при этом возможность взаимодействия, практически невозможно.

Дискреционная модель Кларка-Вильсона

Модель направлена на обеспечение целостности информации. В данной модели рассматриваются т.н. «тройки целостности», включающие в себя:
- субъект;
- операция, не нарушающая целостность;
- объект;

Согласно данной модели, всё множество объектов разделяется на два типа:
- объекты, требующие контроля целостности;
- объекты, не требующие контроля целостности;

Вводятся логически объединенные совокупности элементарных операций, называющиеся процедурами преобразования, а также дополнительный класс процедур, которые обеспечивают проверку целостности. В случае если результаты процедуры преобразования при применении к ним процедур проверки целостности дают положительный результат, они называются «корректно сформированными транзакциями».

Вводятся следующие правила:
- множество процедур проверки целостности должно применяться ко всем объекта, требующим контроля целостности;

- все процедуры преобразования должны быть транзакциями, не нарушающими целостность объектов, и должны применяться только к списку объектов, требующих контроля целостности, устанавливаемых администратором системы;
- система должна контролировать применимость операций к объектам в соответствии со списком, определенным в предыдущем правиле;
- система должна содержать список процедур, разрешенным конкретным пользователям;
- система должна аутентифицировать всех пользователей, выполняющих операции;
- каждая процедура преобразования должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины обстоятельств применения данной процедуры;
- некоторые процедуры преобразования могут превращать объекты, не требующие контроля целостности в объекты, требующие контроля целостности;
- только специально уполномоченный субъект имеет право изменять списки допустимых объектов и процедур преобразования. Данный субъект не имеет права выполнять какие-либо действия, если он уполномочен изменять регламентирующие эти действия списки.

Данная модель является простой в реализации, однако решает только проблему нарушения целостности, потому ее использование не является целесообразным в системах, где важным критерием безопасности является защита конфиденциальности. Наличие списков допустимых операций и объектов позволяет считать систему, основанную на данной модели, гибкой в настройке. По причине изолированности администратора от пользователей, система также является простой в администрировании [6].

Модель Кена Биба

Данная модель является инвертированной версией модели Белла-Лападулы, призванной решать проблемы нарушения целостности.

Ее основными элементами являются:
- множество субъектов;
- множество объектов;
- множество операций над объектами;
- решетка уровней целостности;
- множество состояний системы;
- функции перехода;
- множество наборов запросов.

В отличие от модели Белла-Лападулы, критерий безопасности заключается в недопустимости потоков от субъектов нижних уровней иерархии к объектам верхних уровней, т.к. такие потоки могут нарушить целостность объектов верхних уровней. Основными правилами доступа являются:
- нет записи вверх, т.к. может произойти нарушение целостности объекта;
- нет чтения вниз, т.к. может произойти нарушение целостности субъекта [7].

Данная модель предусматривает понижение уровня целостности субъекта до уровня целостности объекта вместо невозможности чтения вниз, а также автоматическое понижение уровня целостности объекта до уровня целостности субъекта вместо невозможности записи вверх.

Таким образом, модель Кена Биба является противоположной версией модели Белла-Лападулы и обладает теми же преимуществами и недостатками.

Модель Миллена распределения ресурсов

Данная модель направлена на защиту от нарушения доступности информации, ее основная идея заключается в формировании требований к распределению пространства и времени для процессов.

Основными элементами системы являются:
- P — множество активных процессов;
- R — множество пассивных ресурсов;
- c — некоторая фиксированная граница, используемая для обозначения общего максимального числа единиц всех типов ресурсов, доступных в исследуемой системе;
- A_p — вектор распределения, обозначающий для каждого ресурса число единиц ресурсов, выделенных для процесса p в некотором состоянии;
- CPU– особый вид ресурсов, необходимый для формирования информации о том, является ли процесс текущим или застывшим, так если $A_p(CPU) = 1$, то истинным является running(p), иначе истинным является asleep(p);
- Q_p^s — вектор пространственных требований, означающий число единиц каждого ресурса, требуемое процессом p для выполнения необходимого задания в некотором состоянии;
- $T(p)$– функция, обозначающая, когда в последний раз изменились часы для процесса с целью отражения реального времени;
- Q_p^t — вектор временных требований, который обозначает объем времени, необходимого каждому ресурсу процесса p для выполнения работы [8].

Таблица 1. Сводная таблица по результатам анализа

Модель безопасности	Простота реализации	Простота администрирования	Избыточность прав доступа	Гибкость	Защита К	Защита Ц	Защита Д
Модель невмешательства	-	-	-	-		-	-
Модель невыводимости	-	-	-	-	+	-	-
Модель Кларка — Вильсона	+	+	+	+	-	+	-
Модель Биба	+	+	-	-	-	+	-
Модель Миллена	-	-	+	-	-	-	+
Модель Лендвера	-	+	+	+	+	+	-

Предполагается, что процессы могут определять множество ресурсов, необходимых им для завершения работы, до того, как они ее начнут, также предполагается, что процесс может определять временные требования для конкретного задания.

Модель предполагает использование восьми правил, направленных на формирование требований к пространственно-временным характеристикам процесса и потребляемым им ресурсом.

Реализация данной модели при проектировании информационной системы, а также администрирование системы безопасности являются весьма трудоемкими процессами благодаря введению большого количества интуитивно непонятных правил. Система также не является гибкой в настройке по причине явного задания требований и невозможности их изменения.

Модель Лендвера

Данная модель направлена на защиту от нарушения конфиденциальности. Модель Лендвера основана на дискреционной и мандатной политиках доступа. Правилами безопасности являются:

- уровни безопасности, уровней доверия и множество ролей присваивает администратор;
- в пределах уровня безопасности пользователь классифицирует сообщения и определяет набор доступа для сущностей, которые он создаёт, так что только пользователь с требуемой благонадёжностью может просматривать информацию;
- пользователь должным образом контролирует информацию объектов, требующих благонадёжности.

В качестве ограничений безопасности выделяются:

- пользователь может запрашивать операции над сущностями, только если пользовательский идентификатор или текущая роль присутствует в множестве доступа сущности вместе с этой операцией;
- уровень безопасности контейнера всегда больше или равен уровня безопасности сущностей, которые он содержит;
- информация, переносимая из объекта, всегда содержит уровень безопасности объекта. Информация, вставляемая в объект, должна иметь уровень безопасности ниже уровня безопасности этого объекта.
- пользователь может просматривать только объекты с уровнем безопасности меньше, чем уровень безопасности устройства вывода и степень доверия к пользователю;
- пользователь может получить доступ к косвенно адресованной сущности внутри объекта, требующего степени доверия, только если его степень доверия не ниже уровня безопасности контейнера;
- сущности, просмотренные пользователем, должны быть помечены его степенью доверия;
- никакая классифицированная информация не может быть понижена в уровне своей классификации за исключением случая, когда эту операцию выполняет пользователь с ролью «пользователь, уменьшающий классификацию информации»;
- операция уничтожения информации производится только пользователем с ролью «пользователь, уничтожающей информацию».

Исходя из объединения двух политик безопасности сразу, данная модель объединяет многие их преимущества и недостатки. Так, например, система является гибкой, простой в администрировании, однако она сложна в реализации. С другой стороны, возможность задания явных прав доступа и меток безопасности одновременно — решает проблемы нарушения как целостности, так и конфиденциальности.

Результаты

Сводная таблица по результатам анализа выглядит следующим образом:

В ходе исследования были найдены модели, позволяющие, по мнению авторов, решить проблемы классических моделей безопасности.

Исходя из таблицы, можно сделать вывод о том, что практически все проанализированные модели решают проблему защиты только одного свойства безопасности информации. Для использования в информационных системах, где необходимо контролировать защиту нескольких свойств информации, предлагаются следующие подходы:

- совместное использование нескольких моделей безопасности путем слияния их правил и элементов в одну модель;
- совместной использование нескольких моделей безопасности параллельно в рамках одной ИС;
- разработка модели доступа, направленной на защиту нескольких свойств информации одновременно.

Предлагаемые походы следует выбирать исходя из текущих задач ИС, возможности реализации процессов объединения моделей, а также наличия возможности слияния моделей в рамках их функциональных задач.

Среди проанализированных моделей наиболее приоритетной в части защиты конфиденциальности при разработке ИС специального назначения является модель Лендвера, основным недостатком которой является сложность реализации. В случае если защита конфиденциальности информации не является приоритетным направлением в защите ИС, предлагается использовать модель Кларка Вильсона.

Исходя из анализа, в настоящее время существует малое количество моделей безопасности, направленных на решение проблемы защиты доступности информации. Как следствие приоритетными направлениями дальнейших исследований являются изучение возможностей разработки моделей, решающих проблемы защиты трех свойств информации одновременно.

Наиболее оптимальным решением при проектировании ИС, в которой важны процессы сохранения конфиденциальности и целостности информации, является использование модели Лендвера или совместное использование моделей Белла-Лападулы и Биба.

ЛИТЕРАТУРА

1. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005
2. Steve Demurjian: Implementation of Mandatory Access Control in Role-based Security System. 2001
3. Оленников Е.А. и др. Разработка типовой модели управления доступом для типовой медицинской информационной системы: Программные продукты и системы/Software & Systems, № 1 (113), 2016. с. 166–168.
4. Девянин П. Н. Модели безопасности компьютерных систем: М.: Изд.центр «Академия», 2005.— 144 с.
5. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах.— Екатеринбург: изд-во Урал. Ун-та, 2003.— 328 с
6. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С. В.— 2001–352 с
7. Biba, K. J. "Integrity Considerations for Secure Computer Systems"
8. J.Millen "Resource allocation model for denial of service", IEEE simposium on research in security and privacy, 1992.

Журнал «Современная наука: актуальные проблемы теории и практики»