УДК 004.056.53

ПОЛИТИКА УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ СИСТЕМЫ ОБРАБОТКИ ГЕОЛОГО-ГЕОФИЗИЧЕСКИХ ДАННЫХ

Кругликов С.В.[1], Дмитриев В.А.[2], Степанян А.Б.[3], Максимович Е.П.[4]

Статья посвящена *вопросам использования в системах защиты информации информационных систем совокупности разных моделей управления доступом, в том числе стандартных моделей мандатного, дискреционного и ролевого разграничения доступа. Анализируется эффективность применения каждой из этих моделей для обеспечения защиты от несанкционированного доступа к информации. Показано, что по отдельности они не обеспечивают необходимого уровня защиты, а интегрирование нескольких различных моделей предоставляет возможность уменьшить уязвимости, связанные с получением несанкционированного доступа, и противостоять угрозам безопасности информационной системе.*

Ключевые слова: *управление доступом мандатное, управление доступом дискреционное, управление доступом ролевое, управление информационными потоками.*

DOI: 10.21681/2311-3456-2018-3-XX-YY

Введение

Геолого-геофизические данные относятся к данным ограниченного распространения и требуют обеспечения их конфиденциальности, целостности и доступности в процессе обработки, хранения и передачи по каналам связи [1, 2]. Это обусловливает актуальность создания системы защиты информации (СЗИ) многопользовательской высокопроизводительной информационно-вычислительной системы обработки геолого-геофизических данных (ИС ОГГД).

Одним из ключевых аспектов создания СЗИ любой информационной системы (ИС) является определение и реализация эффективной политики управления доступом [3-5]. В статье приводятся результаты исследований, проделанных в этом направлении в ходе проектирования и создания СЗИ ИС ОГГД.

Совмещение нескольких политик разграничения доступа в ИС ОГГД является эффективным средством безопасности, реализация которого представляет собой актуальную проблему создания системы защиты информации и практического администрирования ИС ОГГД. Использование нескольких различных моделей разграничения доступа предоставляет возможность расширить круг перекрываемых путей утечки информации и преодолеть многие недостатки, присущие отдельным моделям [6].

Анализ базовых моделей управления доступом

На начальном этапе выполнения работ по определению политики управления доступом был проведен предварительный анализ основных моделей управления доступом: MAC (Mandatory Access Control) – модели мандатного управления доступом, DAC (Discretionary access control) – модели дискреционного управления доступом и RBAC (Role-Based Access Control) – модели ролевого управления доступом [3, 4, 7-9].

Пусть O – множество объектов доступа ИС, S – множество субъектов доступа ИС ($S \subseteq O$), P – множество прав доступа.

Мандатное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Права доступа объектов и субъектов определяются двумя компонентами: уровень секретности объектов и субъектов и множество категорий (список имен тематических областей, к которым принадлежит объект). Вводится решетка уровня секретности с отношением доминирования (L, ≤), где L = {U (unclassified), C (confidential), S (secret), TS (top secret)) и U<C<S<TS.

Критерий безопасности состоит в том, что субъект может читать информацию из объекта только тогда, когда уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Данный критерий фактически означает запрет определенных информационных потоков, которые трактуются как опасные и недопустимые, а также изоляцию пользователей и процессов, как известных, так и неизвестных системе.

Для анализа систем защиты, реализующих мандатное разграничение доступа, предназначена модель Белла-ЛаПадулы, рассматривающая условия, при выполнении которых в ИС невозможно возникновение информационных потоков от объектов с большим уровнем конфиденциальности к субъектам с мень-

1 Кругликов Сергей Владимирович, доктор военных наук., Объединенный институт проблем информатики Национальной академии наук Беларусии, г. Минск, Белоруссия. E-mail: kruglikov_s@newman.bas-net.by

2 Дмитриев Владимир Александрович, кандидат физико-математических наук, Объединенный институт проблем информатики Национальной академии наук Беларусии, г. Минск, Белоруссия. E-mail: vladdmitr@newman.bas-net.by

3 Степанян Арарат Баркевович, кандидат технических наук, Объединенный институт проблем информатики Национальной академии наук Беларусии, г. Минск, Белоруссия. E-mail: ararat@newman.bas-net.by.

4 Максимович Елена Павловна, кандидат физико-математических наук, Объединенный институт проблем информатики Национальной академии наук Беларусии, г. Минск, Белоруссия. E-mail: maksimovich@newman.bas-net.by

шим уровнем конфиденциальности. Вводятся специальные правила проверки прав доступа NO-READ-UP, запрещающего чтение файлов, имеющих уровень секретности больше, чем уровень доступа субъекта, и NO-WRITE-DOWN, запрещающего «рассекречивать» информацию, т.е. записывать информацию в файлы, имеющие меньший уровень секретности, чем текущий уровень субъекта.

На основе концепции MAC разработана также модель Биба, реализующая контроль целостности данных путем добавления к субъектам и объектам уровня целостности и запрета общения субъектов и объектов разных уровней. Действуют правила: NO-WRITE-UP – запрет записи данных в файлы, имеющие более высокий уровень целостности и NO-READ-DOWN – запрет чтения информации из менее целостных файлов.

Модель мандатного управления доступом задает жесткую систему управления доступом и обычно пользователю не разрешается устанавливать более свободный доступ даже к своим ресурсам. В сравнении с дискреционным управлением доступом модель MAC предотвращает утечку конфиденциальной информации, но не обладает достаточной гибкостью.

Дискреционное управление доступом DAC определяется двумя основными свойствами:

– все субъекты и объекты идентифицированы;

– права доступа субъектов к объектам определяются на основании принятых в системе правил.

Ключевым элементом модели DAC является матрица доступа $M=(M_{so})_{s\in S, o\in O}$, $M_{so}\subseteq P$. Основные операции, предусмотренные данной моделью: Grant (внести разрешение в нужную ячейку M), Revoke (удалить разрешение из ячейки), Check (проверить, есть ли требуемое разрешение в определенной ячейке M).

Модель отличается простотой реализации, но не обеспечивает надлежащего уровня защищенности. В частности, DAC уязвима к атаке типа «Троянский конь» поскольку в ней контролируются только операции доступа субъектов к объектам, а не потоки информации между ними (пользователь может случайно или преднамеренно передать доступ неавторизованным пользователям) [10]. В случае DAC трудоемкость администрирования ИС очень чувствительна к количеству пользователей (например, в части поддержки оперативного изменения прав доступа в формируемой вручную матрице доступа и др.).

Поведение системы может моделироваться как последовательность состояний, описываемых совокупностью субъектов, объектов и матрицей доступа. Критерий безопасности системы в состоянии Q_0 заключается в том, что не существует такой последовательности команд, в результате выполнения которых в некоторую ячейку матрицы доступа M будет занесено право p, отсутствующее в состоянии Q_0 (критерий Харрисона-Руззо-Ульмана).

В рамках политики DAC возникает задача проверки того могут ли действия субъекта, выполняемые в соответствии с установленными правами доступа привести к нарушению безопасности ИС. Для анализа системы защиты, реализующей DAC, разработана модель Харрисона–Руззо–Ульмана (HRU). Как показывают результаты ее анализа, задача построения алгоритма проверки безопасности систем, реализующих DAC, не может быть решена в общем случае. Задача проверки безопасности произвольных систем алгоритмически неразрешима. Хотя имеются некоторые модели ИС, реализующих DAC (например, модель Take-Grant, ориентированная на анализ путей распространения прав доступа), которые предоставляют алгоритмы проверки безопасности, но данный класс систем слишком узкий. Так как в общем случае политика DAC не позволяет реализовать четкую гарантированную систему защиты информации ИС, актуальна разработка более совершенных подходов (в том числе и на основе сочетания DAC с другими типами политик разграничения доступом).

Механизмы реализации дискреционной модели доступа в Windows предусматривают включение в объекты разграничения доступа дескриптора безопасности, содержащего информацию о владельце объекта (его идентификаторе безопасности SID, Security Identifier) и дискреционном списке управления доступом к объекту (Discretionary Access Control List, DACL), правом редактирования которого обладают владелец объекта и администратор. Права доступа к объектам в операционной системе Windows делятся на специальные, стандартные (общие) и родовые (generic). Специальные права зависят от типа объекта разграничения доступа. Стандартные права доступа к объектам операционной системы Windows не зависят от типа объекта. Каждое из родовых разрешений представляет собой логическую группу специальных и стандартных разрешений. Назначение и управление правами доступа облегчает механизм наследования. Например, файлы, создаваемые в папке, наследуют разрешения этой папки. В Linux индекс файла содержит информацию о владельце файла (его идентификаторе, User Identifier, UID), его первичной группе (идентификаторе группы, Group Identifier, GID) и векторе доступа к файлу. В рамках ограничения доступа к объектам используются дополнительные биты доступа: SUID (бит в подвекторе прав владельца, обеспечивающий выполнение файла с правами не пользователя, а владельца файла), SGID (бит в подвекторе прав членов группы владельца файла, обеспечивающий выполнение файла с правами не пользователя, а членов группы владельца файла), Sticky (бит в подвекторе прав всех остальных пользователей, запрещающий удаление и переименование в общем каталоге файлов, созданных другими пользователями).

В ряд современных серверных операционных систем Windows и Linux включена поддержка ролевого разграничения доступа.

Ролевая модель RBAC основана на присвоении пользователям ролей, представляющих собой множество разрешенных функций. Целью использования ролевой модели доступа является предоставление пользователю прав доступа только к объектам необходимым для исполнения данной роли.

Основными элементами базовой модели RBAC являются:

– U – множество пользователей;

– R – множество ролей;

– P– множество прав доступа на объекты ИС;

– C – множество сессий пользователей;

– PA: $R\rightarrow 2^P$ – отображение, определяющее для каждой роли множество прав доступа; при этом для каждого $p\in P$ существует $r\in R$ такая что $p\in PA(r)$;

– UA: $U \rightarrow 2^R$ – отображение, определяющее для каждого пользователя множество ролей, на которые он может быть авторизован;

– user: $C \rightarrow U$ – отображение, определяющее для каждой сессии пользователя, от имени которого она активирована;

– roles: $C \rightarrow 2^R$ – отображение, определяющее для пользователя множество ролей, на которые он авторизован в данной сессии; при этом в каждой момент времени для каждой $c \in C$ выполняется условие roles(c) $\subseteq UA$(user(c)).

В рамках осуществления ролевого управления доступом надо учитывать, что реализация возможности работы пользователя под одной учетной записью в различных ролях является потенциально опасным решением, так как при необходимости выполнения требования к разграничению прав доступа к информации, обрабатываемой в различных ролях создаются дополнительные каналы несанкционированного обмена информацией между ролями.

В терминах ролевой модели легко реализуется принцип минимальной (общедоступной) привилегии. Ролевое разграничение доступа позволяет реализовать гибкие, динамически изменяющиеся в процессе функционирования ИС правила разграничения доступа. Модель RBAC целесообразно использовать в ИС больших организаций, со сложной иерархией и большим количеством разделяемых операций. В этом случае данные обычно принадлежат не пользователю, а системе, и управление доступом к ресурсам основывается не на принадлежности ресурса, а на функциях пользователя в организации. Однако при использовании ролевой модели возникают трудности, связанные с наличием ролевых иерархий и наследования, а также с контролем безопасного состояния системы.

Таким образом, каждый из классических методов разграничения доступа, реализованных в рамках ОС и СУБД, имеет свои преимущества и недостатки [11-16]. Использование только одного из них оказывается недостаточным для эффективного и надежного функционирования распределенных систем обработки данных с большим количеством объектов (данных) разных категорий доступа и субъектов, требующих назначения разных прав доступа.

Совмещение нескольких политик управления доступом

Проблема сочетания разных политик управления доступом в рамках одной информационной системы связана с необходимость решения целого ряда задач, таких как выбор «базиса», на котором будут основаны используемые модели; определение совокупности используемых политик безопасности, которые описывают правила доступа; внедрение дополнительных механизмов разграничения доступа в системное обеспечение; практическое использование и администрирование таких механизмов в составе программных комплексов; обеспечение отслеживания и определения потенциально небезопасных состояний системы; определение приоритетов использования политик управления доступом; разработка специальных инструментов управления политиками разграничения доступа, осуществляющих выбор политики доступа при конкретном запросе на доступ и многие другие.

Совместно используемые модели доступа не должны противоречить друг другу. В ряде случаев возникающие конфликты могут разрешаться, например, на уровне администрирования информационной системы.

В качестве примера совмещения политик доступа можно привести системы управления базами данных, функционирующие на базе операционных систем семейств Windows, Linux. В системах управления базами данных наиболее распространенной является ролевая политика безопасности, но при этом данные хранятся в файлах, доступ к которым разграничивается операционной системой. В операционных системах базовой чаще всего является модель дискреционного или мандатного управления доступом. Политика дискреционного или мандатного разграничения доступа обычно используется также при реализации политики безопасности информационных потоков информационной системы.

В целях расширения возможностей ролевой политики RBAC может использоваться атрибутное управление доступом ABAC (attribute based access control) – метод управления доступом, в котором решение на предоставление или отклонение доступа субъекту на выполнения операции над объектами основывается на назначенных субъекту и объекту атрибутах, а также условиях окружающей среды и наборе политик, указанных в этих атрибутах и условиях [3, 17-20]. Это может добавить определенные ограничения, касающиеся элементов модели (ограничение количества членов конкретной роли, невозможность одновременного назначения определенных ролей одному лицу, ужесточение прав доступа пользователей в нерабочее время, удаленного доступа по мобильному устройству и т.д.). Права доступа пользователей могут зависеть не только от их роли, но и от местонахождения (например, ограничиваются только тем сегментом базы данных, который касается определенного региона). Атрибут «местоположение» может определять либо место формирования запроса на операцию, либо место выполнения операции, либо то и другое. Применение таких атрибутов может основываться на внутренних таблицах для сопоставления логических интерфейсов функций безопасности с местами расположения терминалов, процессоров и т. д. Функции управления доступом должны предоставлять возможность явно предоставлять или запрещать доступ к объектам на основании атрибутов безопасности. Кроме того, должен быть реализован механизм, направленный на исключение конфликтов ролей, которые могут возникать из-за того, что пользователь в результате авторизации получает права от несовместимых ролей. Для этого применяется разбиение ролей на взаимоисключающие множества. Подобные комбинации методов позволяют реализовать более гибкие, понятные и легкоуправляемые методы управления доступом.

Примером формальной модели, эффективно сочетающей дискреционное, мандатное и ролевое управление доступом с учетом безопасности информационных потоков, является мандатная сущностно-ролевая ДП-модель управления доступом и информационными

потоками [16, 21, 22]. Эта модель успешно реализована в защищенной ОС Astra Linux SE и учитывает не только единичный акт доступа к данным, но и направления распространения потоков информации при выполнении операций над данными (с целью предупреждения неконтролируемого распространения прав доступа и возможности создания запрещенных информационных потоков) [16]. Традиционный подход (уровни конфиденциальности, категории безопасности) мандатной модели усиливается применением контроля целостности (управления уровнем доверия). Реализован учет иерархичности организации ряда объектов доступа и функций (ролей) субъектов. Подобные объекты и роли могут быть отнесены к единой категории «сущность», в рамках которой могут формироваться отношения иерархии. Иерархия сущностей позволяет определять правила размещения обычных объектов-сущностей с разными мандатными метками и уровнями целостности в сущности-контейнере (каталоге) с определенными мандатной меткой и уровнем целостности. С помощью введения дополнительных атрибутов ограничивается возможность размещения в контейнерах объектов с мандатными метками и уровнями целостности, которые превышают таковые у самого контейнера.

Политика управления доступом к ресурсам ИС ОГГД

В соответствии с проведенным анализом существующих моделей управления доступом и с учетом специфики ИС ОГГД была определена и реализована политика управления доступа к ресурсам ИС ОГГД, сочетающая в себе дискреционную и ролевую модели управления доступом, атрибутное управление доступом на основании механизмов управления доступом. Данные механизмы обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивают контроль соблюдения этих правил. СЗИ обеспечивает предоставление субъекту только тех ресурсов системы, которые обусловлены установленными правилами разграничения доступа, и запрещает доступ к соответствующим ресурсам при выходе за пределы любого из установленных ограничений. Описание политик управления доступом базируется на стандарте XACML, определяющем базовую схему для выражения правил предоставления прав доступа в формате XML для различных устройств и приложений.

Для определения допустимости операции управляемого субъекта на управляемом объекте в ходе функционирования ИС обеспечено выполнение следующих стандартных действий:

– предоставление доступа к информации и сервисам ИС ОГГД только после проведения процедур идентификации и аутентификации (с использованием механизмов однократной аутентификации и делегирования);

– проверяется правомочность доступа субъекта к объекту;

– определяются операции над объектом, разрешенные для субъекта;

– инициируется выполнение операции субъекта над объектом, если данная операция для субъекта разрешена, в противном случае операция отклоняется с выдачей субъекту предупреждающего сообщения (кода).

Защита от несанкционированного доступа к ресурсам ИС ОГГД обеспечивается применением технических, системных и прикладных методов обеспечения безопасности. Технические методы заключаются в использовании межсетевых экранов, обеспечивающих пропуск запросов по определенным протоколам. Системные методы заключаются в установке, настройке и использовании средств криптографической поддержки, установке, настройке и использовании ОС и СУБД. Прикладные методы реализованы в модулях ИС ОГГД, осуществляющих операцию идентификации и аутентификации пользователей.

Доступ к ресурсам ИС ОГГД производится на основании проверки действительности сертификата пользователя, с применением криптографического протокола.

Доступ к секретным ключам идентификации (шифрования) осуществляется средствами криптопровайдера на основе политики дискреционного управления – только после успешной аутентификации (ввода пароля) владельцем ключей.

Для ИС ОГГД предусмотрен удаленный доступ зарегистрированных пользователей на основе использования технологии «клиент-сервер» и формирования внешних вызовов для получения авторизованного доступа к ресурсам ИС ОГГД. Клиентская часть должна соответствовать требованиям Технического регламента РБ ТР 2013/027/BY[5].

В рамках управления доступом пользователей предусмотрены следующие операции: создание пользователя, удаление пользователя, назначение и корректировка прав пользователя, смена пароля пользователя, создание новой роли, добавление роли, удаление роли, корректировка роли, включение функции в роль, исключение функции из роли.

Для защиты от несанкционированного доступа к ресурсам ИС ОГГД используется также политика сетевого экранирования и управления информационными потоками для субъектов, данных и операций по пересылке управляемой информации к управляемым субъектам и от них. Данная политика осуществляется на основе следующих видов атрибутов безопасности субъектов и данных: сетевые реквизиты отправителя, сетевые реквизиты получателя, тип запрашивающего сервиса (порт отправителя), тип запрашиваемого сервиса (порт получателя), а также некоторые другие, специально определенные атрибуты безопасности субъектов и данных.

Выводы

Для сложных многокомпонентных систем часто эффективно использовать политику разграничения до-

5 ТР 2013/027/BY Информационные технологии. Средства защиты информации. Информационная безопасность. Мн.: Госстандарт, 2013. 7 с.

ступом, основанную на сочетании нескольких моделей управления доступом.

При создании обшей модели управления доступом на основе взаимодействия нескольких моделей разграничения доступа необходимо учесть следующие аспекты:

– принципы работы (правила управления доступом) каждой модели в целях построенной общей архитектуры управления доступом и выражение моделей контроля доступа в унифицированных терминах;

– определение настроек, критериев, которые для каждого запроса на доступ определяют, какая политика безопасности будет задействована;

– поддержка согласованности и непротиворечивости созданной модели в зависимости от соответствующих структур данных ИС;

– порядок применения разных моделей разграничения доступа (последовательно, параллельно, циклично и др.);

– отслеживание проблем, связанных с определением безопасного состояния системы, при построении политик.

Примером практической реализации политики управления доступом, сочетающей ролевую и дискреционную модели доступа, является СЗИ ИС ОГГД, созданная в рамках выполнения научно-технической программы Союзного государства «СКИФ-НЕДРА» [23, 24].

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Исаев В.И. Банк геолого-геофизических данных - информационно-аналитическая основа прогнозирования нефтегазоносности // Известия Томского политехнического университета. 2002. Т. 305. № 6. С. 198-209.
2. Zhu Y., Tan Y., Luo X., He Z. Big Data Management for Cloud-Enabled Geological Information Services. Scientific Programming. 2018. V. 2018, P. 1327214. DOI: 10.1155/2018/1327214.
3. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий. - М.: ДМК Пресс, 2017. 224 с.
4. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия – Телеком, 2017. 338 с.
5. Hwang J., Lee D.Y., Williams L., Vouk M. Access Control Policy Evolution: An Empirical Study. In Proc. 25th IEEE Int'l Symp. on Software Reliability Engineering (ISSRE '14), 2014, pp. 245–254. DOI: 10.1109/ISSRE.2014.36.
6. Лапин С.А. Сравнительный анализ использования существующих моделей разграничения доступа в системах, обладающих равнозначными объектами // Известия Алтайского государственного университета. 2016. № 1 (89). С. 142-147.
7. Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60-68.
8. Mammass M., Ghadi F., An Overview on Access Control Models, International Journal of Applied Evolutionary Computation, 2015, vol. 6, pp. 28.
9. Masood R., Shibli M.A. Comparative Analysis of Access Control Systems on Cloud. In Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD), 2012 13th ACIS International Conference, 2012, pp. 41-46.
10.Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, Технологии, Протоколы. 5-е изд. – СПб.: Питер, 2016. - 991 с.
11. Бойченко И.А., Сарайкин В.Г. Интегрированная модель политик безопасности в СУБД // Известия высших учебных заведений. Лесной журнал. 2005. № 5. С. 132-138.
12. Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем // Труды Института системного программирования РАН. 2017. Т. 29. № 3. С. 7-16.
13. Ефанов Д.В., Рощин П.Г. Метод взаимодействия графических приложений с сессионными службами D-Bus в операционной системе с многоуровневым управлением доступом // Проблемы информационной безопасности. Компьютерные системы. 2015. № 1. С. 34-45.
14. Колегов Д.Н., Ткаченко Н.О., Чернов Д.В. Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL // Прикладная дискретная математика. Приложение. 2013. № 6. С. 62-67.
15. Попов В. ОС И СУБД: Мандатное разграничение доступа // Открытые системы. СУБД. 2017. №1. С. 19-21.
16. Шумилин А.В. Основные элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в СУБД PostgreSQL ОС специального назначения Astra Linux Special Edition // Прикладная дискретная математика. 2013. № 3(21). С. 52–67.
17. Чернов Д.В. О моделях логического управления доступом на основе атрибутов // Прикладная дискретная математика. Приложение. 2012. № 5. С. 79-82.
18. Hu V.C. and etc. Guide to attribute based access control (ABAC) definition and considerations, NIST Spec. Publ., 2014, vol. 800, p. 162.
19. Hu V.C. and etc. Attribute-Based Access Control // Computer (Long. Beach. Calif)., 2015, vol. 48, no. 2, pp. 85–88.
20. Xu D., Zhang Y. Specification and analysis of attribute-based access control policies: An overview. In Proc. - 8th Int. Conf. Softw. Secur. Reliab. - Companion, SERE-C 2014, 2014, pp. 41–49.
21. Девянин П.Н. Ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux // Прикладная дискретная математика. 2012. № 1 (15). С. 69-90.
22. Тележников В.Ю. Правила преобразования состояний системы в рамках ДП-модели управления доступом в компьютерных сетях, построенных на основе ос семейства Linux // Прикладная дискретная математика. 2016. № 1 (31). С. 67-85.
23. Гудзева А.В., Томакова И.А. Направления сотрудничества в наукоемких отраслях промышленности в рамках союзного государства России и Белоруссии // Инновационные процессы и технологии в современном мире. 2016. № 1 (4). С. 173-176.
24. Юсупов Р.М., Жаворонкин О.В. Выбор технологического направления создания высокопроизводительных информационно-вычислительных систем управления геолого-геофизическими данными (в рамках программы «СКИФ-НЕДРА»). В сборнике: Вопросы теории и практики геологической интерпретации геофизических полей Материалы 43-й сессии Международного научного семинара им. Д. Г. Успенского. 2016. С. 190-192.

POLICY OF DISTINCTION ACCESS TO INFORMATION SECURITY SYSTEM OF HIGH-PERFORMANCE PROCESSING SYSTEM OF GEOLOGICAL-GEOPHYSICAL DATA

Kruglikov S.V.[6], Dmitriev V.A.[7], Stepanian A.B.[8], Maksimovich E.P.[9]

The article focuses *on the use of a variety of different access control models in information security systems, including standard models of mandatory, discretionary and role-based access control. The effectiveness of each of these models is analyzed to provide the protection against unauthorized access to information. It is shown that individually they do not provide the required level of protection, and the integration of several different models makes it possible to reduce the vulnerabilities due to of unauthorized access and to oppose the threats to the security of the information system.*

Keywords: *Mandatory access control, discretionary access control, access control role-based, management of information flows*

References

1. Isaev V.I. Bank geologo-geofizicheskih dannyh - informacionno-analiticheskaya osnova prognozirovaniya neftegazonosnosti. Izvestiya Tomskogo politekhnicheskogo universiteta. 2002. T. 305. N 6. S. 198-209.
2. Zhu Y., Tan Y., Luo X., He Z. Big Data Management for Cloud-Enabled Geological Information Services. Scientific Programming. 2018. V. 2018, P. 1327214. DOI: 10.1155/2018/1327214.
3. Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem› bezopasnyh informacionnyh tekhnologij. - M.: DMK Press, 2017. 224 s.
4. Devyanin P.N. Modeli bezopasnosti komp›yuternyh sistem. Upravlenie dostupom i informacionnymi potokami. Uchebnoe posobie dlya vuzov. 2-e izd., ispr. i dop. M.: Goryachaya liniya – Telekom, 2017 g.338 str
5. Hwang J., Lee D.Y., Williams L., Vouk M. Access Control Policy Evolution: An Empirical Study. In Proc. 25th IEEE Int'l Symp. on Software Reliability Engineering (ISSRE '14), 2014, pp. 245–254. DOI: 10.1109/ISSRE.2014.36.
6. Lapin S.A. Sravnitel›nyj analiz ispol›zovaniya sushchestvuyushchih modelej razgranicheniya dostupa v sistemah, obladayushchih ravnoznachnymi ob»ektami. Izvestiya Altajskogo gosudarstvennogo universiteta. 2016. N 1 (89). S. 142-147.
7. Markov A.S., Cirlov V.L. Bezopasnost› dostupa: podgotovka k CISSP. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. N 2 (10). S. 60-68. DOI: /10.21681/2311-3456-2015-2-60-68.
8. Mammass M., Ghadi F., An Overview on Access Control Models, International Journal of Applied Evolutionary Computation, vol. 6, pp. 28, 2015.
9. Masood R., Shibli M.A. Comparative Analysis of Access Control Systems on Cloud. In Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD), 2012 13th ACIS International Conference. 2012, pp. 41-46.
10. Olifer V.G., Olifer N.A. Komp›yuternye seti. Principy, Tekhnologii, Protokoly. 5-e izd. – SPb.: Piter, 2016. - 991 s.
11. Bojchenko I.A., Sarajkin V.G. Integrirovannaya model› politik bezopasnosti v SUBD. Izvestiya vysshih uchebnyh zavedenij. Lesnoj zhurnal. 2005. N 5. S. 132-138.
12. Devyanin P.N. O probleme predstavleniya formal›noj modeli politiki bezopasnosti operacionnyh sistem. Trudy Instituta sistemnogo programmirovaniya RAN. 2017. T. 29. N 3. S. 7-16.
13. Efanov D.V., Roshchin P.G. Metod vzaimodejstviya graficheskih prilozhenij s sessionnymi sluzhbami D-Bus v operacionnoj sisteme s mnogourovnevym upravleniem dostupom. Problemy informacionnoj bezopasnosti. Komp›yuternye sistemy. 2015. N 1. S. 34-45.
14. Kolegov D.N., Tkachenko N.O., CHernov D.V. Razrabotka i realizaciya mandatnyh mekhanizmov upravleniya dostupom v SUBD MySQL. Prikladnaya diskretnaya matematika. Prilozhenie. 2013. N 6. S. 62-67.
15. Popov V. OS I SUBD: Mandatnoe razgranichenie dostupa. Otkrytye sistemy. SUBD. 2017. N1. S. 19-21.
16. SHumilin A.V. Osnovnye ehlementy mandatnoj sushchnostno-rolevoj DP-modeli upravleniya dostupom i informacionnymi potokami v SUBD PostgreSQL OS special›nogo naznacheniya Astra Linux Special Edition. Prikladnaya diskretnaya matematika. 2013. N 3(21). S. 52–67.
17. CHernov D.V. O modelyah logicheskogo upravleniya dostupom na osnove atributov. Prikladnaya diskretnaya matematika. Prilozhenie. 2012. N 5. S. 79-82.
18. Hu V.C. and etc. Guide to attribute based access control (ABAC) definition and considerations, NIST Spec. Publ., 2014, vol. 800, p. 162.
19. Hu V.C. and etc. Attribute-Based Access Control. Computer (Long. Beach. Calif)., 2015, vol. 48, no. 2, pp. 85–88.
20. Xu D., Zhang Y. Specification and analysis of attribute-based access control policies: An overview. In Proc. - 8th Int. Conf. Softw. Secur. Reliab. - Companion, SERE-C 2014, 2014, pp. 41–49.
21. Devyanin P.N. Rolevaya DP-model› upravleniya dostupom i informacionnymi potokami v operacionnyh sistemah semejstva Linux. Prikladnaya diskretnaya matematika. 2012. N 1 (15). S. 69-90.
22. Telezhnikov V.YU. Pravila preobrazovaniya sostoyanij sistemy v ramkah DP-modeli upravleniya dostupom v komp›yuternyh setyah, postroennyh na osnove os semejstva Linux. Prikladnaya diskretnaya matematika. 2016. N 1 (31). S. 67-85.

6 Sergey Kruglikov, Dr.Sc., United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: kruglikov_s@newman.bas-net.by
7 Vladimir Dmitriev, PhD, United Institute of Informatics Problems of the National Academy of Sciences of Belarus, , Minsk, Belarus. E-mail: vladdmitr@newman.bas-net.by
8 Ararat Stepanian, PhD, United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: ararat@newman.bas-net.by
9 Elena Maksimovich, PhD, United Institute of Informatics Problems of the National Academy of Sciences of Belarus, Minsk, Belarus. E-mail: maksimovich@newman.bas-net.by

23. Gudzeva A.V., Tomakova I.A. Napravleniya sotrudnichestva v naukoemkih otraslyah promyshlennosti v ramkah soyuznogo gosudarstva Rossii i Belorussii. Innovacionnye processy i tekhnologii v sovremennom mire. 2016. N 1 (4). S. 173-176.
24. YUsupov R.M., ZHavoronkin O.V. Vybor tekhnologicheskogo napravleniya sozdaniya vysokoproizvoditel›nyh informacionno-vychislitel›nyh sistem upravleniya geologo-geofizicheskimi dannymi (v ramkah programmy «SKIF-NEDRA»). V sbornike: Voprosy teorii i praktiki geologicheskoj interpretacii geofizicheskih polej Materialy 43-j sessii Mezhdunarodnogo nauchnogo seminara im. D. G. Uspenskogo. 2016. S. 190-192.