Мандатный контроль в автоматизированных информационных системах*

Г. П. Акимова, А. Ю. Даниленко, Е. В. Пашкина, М. А. Пашкин,
А. А. Подрабинович, И. В. Туманова

Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" Российской академии наук", г. Москва, Россия

Аннотация. В статье рассмотрены подходы к управлению доступом и контролю целостности с использованием мандатных алгоритмов. В настоящее время эти подходы к обеспечению информационной безопасности не находят широкого применения при разработке автоматизированных информационных систем вследствие ограничений на их реализацию. Авторами предложено заменить часть таких ограничений рядом правил, которые позволяют точнее учесть деловую логику эксплуатирующих организаций и не противоречат требованиям по обеспечению информационной безопасности. Такой подход позволяет существенно расширить применение мандатного контроля во всех видах информационных систем.

Ключевые слова: информационная безопасность, автоматизированные информационные системы, мандатное управление доступом, мандатный контроль целостности.

DOI 10.14357/20718632200301

Введение

Одним из основных элементов защиты информации в автоматизированных информационных системах (АИС) являются подсистемы управления доступом, в которых наиболее широко применяются алгоритмы дискреционного и ролевого разграничения. Для дискреционного контроля доступа используется понятие матрицы доступа, в этом случае для каждого информационного объекта указывается, какие пользователи АИС имеют права на выполнение каких действий в системе (чтение, модификация, удаление и т.д.), причем обычно такие алгоритмы реализуются путем задания списков доступа для каждого объекта. Списки доступа, в свою очередь, подразделяются на списки разрешений (какие действия каким пользователям разрешены) и списки запретов (какие действия запрещены). Для ролевого разграничения в АИС предусматривается некоторый набор так называемых ролей (администраторы, администраторы безопасности, руководители подразделений и т.д.), каждая из которых имеет определенный набор полномочий. В зависимости от деловой логики системы возможны варианты, когда допускается назначение на одну роль нескольких пользователей или только одного.

Алгоритмы мандатного управления доступом и мандатного контроля целостности в АИС используются существенно реже. Они были разработаны для АИС государственных органов США, работающих с данными разных уровней конфиденциальности, в том числе с секретной информацией [1, 2].

*Работа выполнена при частичной поддержке РФФИ, проект 17-29-03263

Изначальная формулировка мандатной модели управления доступом [1] предусматривала разграничение по уровням секретности и предназначалась для того, чтобы не допустить чтение документов высокого уровня секретности пользователями, уровень допуска которых был ниже требуемого значения. Наиболее адекватное описание современной логики работы в этой части приведено в Руководящем документе [3]:

«Для реализации должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий.

Комплекс средств защиты должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

– субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

– субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта». Отметим, что из приведенной формулировки следует возможность субъекта изменять объект более высокого уровня конфиденциальности, чем его собственный уровень при отсутствии права на чтение этого объекта.

Помимо вышесказанного, согласно [3], требуется обеспечить возможность «изменения классификационных уровней субъектов и объектов специально выделенными субъектами».

Совокупность иерархических и неиерархических категорий пользователя или объекта называется мандатным профилем.

Отметим, что одной из важных особенностей мандатного контроля доступа является его принудительность, т.е. доступ по мандатным профилям проверяется всегда вне зависимости от дискреционных прав как для явного, так и опосредованного обращения пользователя к объектам. Кроме того, в отличие от дискреционных прав доступа, мандатный профиль новых объектов определяется мандатным профилем субъекта, а изменение мандатных профилей самих пользователей и информационных объектов, максимально ограничено. Это ограничение может быть реализовано с помощью разных алгоритмов, например, изменение мандатного профиля пользователя доступно только администраторам безопасности, а изменение профиля объекта может быть полностью запрещено.

Логика работы мандатного контроля целостности основана на понятиях уровня доверия пользователя и уровня ценности обрабатываемого объекта, которые вместе называются уровнями целостности. Классическая модель Биба [2], на которой основаны алгоритмы мандатного контроля целостности, базируется на следующих принципах:

– субъекты на заданном уровне целостности не должны читать данные на более низком уровне целостности (запрет чтения «снизу», политика No-Read-Down);

– субъекты на заданном уровне целостности не должны писать данные на более высоком уровне целостности (запрет записи «наверх», политика No-Write-Up).

Смысл этих правил в том, что запись «наверх» может представлять угрозу, поскольку субъект с низким уровнем безопасности может исказить или уничтожить данные в объекте, лежащем на более высоком уровне. Также можно рассматривать чтение «снизу» как поток информации, идущий из объекта нижнего уровня и нарушающий целостность субъекта высокого уровня. Поэтому весьма вероятно, что и такое чтение целесообразно запретить. Помимо рассмотренных политик No-Read-Down и No-Write-Up могут использоваться политики No-Read-Up (запрет чтения «сверху») и No-Write-Down (запрет записи «вниз»).

Нормативные документы требуют обязательного применения мандатного контроля до-

ступа в ряде конкретных случаев, применение мандатного контроля целостности, как правило, не регламентировано. В частности, в упомянутом Руководящем документе [3] применение мандатного контроля доступа в обязательном порядке требуется для средств вычислительной техники, начиная с четвертого класса защищенности. Однако сам принцип мандатного разграничения может быть использован и в АИС, не обрабатывающих информацию, отнесенную к государственной тайне. В частности, в приказах ФСТЭК [4, 5] предусмотрена «реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа» для АИС, обрабатывающих персональные данные, а также для государственных информационных систем, не обрабатывающих секретную информацию. Таким образом, в этих случаях выбор методов разграничения доступа, подлежащих реализации в АИС, выполняется разработчиками и заказчиками системы, исходя из деловой логики и характеристик обрабатываемых данных. Отметим, что упомянутые выше документы [3-5] не требуют реализации в АИС мандатного контроля целостности.

1. Варианты реализации мандатного контроля

Вопрос проектирования и разработки АИС с поддержкой мандатного разграничения доступа на данный момент чрезвычайно актуален. В [6] приведено описание мандатной модели управления доступом и примеры ее применения в различных АИС. Общие принципы реализации мандатного контроля при автоматизации деятельности научного института описаны в [7]. В [8] приводится описание системы электронного документооборота (СЭД), в которой может быть реализовано мандатное разграничение доступа. В указанных работах отмечается, что разграничение доступа по уровням конфиденциальности может быть реализовано тремя способами: физическим разделением локальной вычислительной сети на контуры, в каждом из которых обрабатывается информация одного уровня; разграничение средствами АИС при условии, что сеансу работы пользователя средствами операционной системы (ОС) присваивается определенный уровень конфиденциальности, наследуемый создаваемыми объектами; разграничение средствами АИС без привязки к свойствам сеанса работы пользователя, степень конфиденциальности информационного объекта определяется самим пользователем. Последний вариант наиболее близок по логике работы к правилам работы с конфиденциальными документами на бумажных носителях.

Мандатный контроль как доступа, так и целостности, реализован в некоторых современных ОС и системах управления базами данных (СУБД).

При этом механизм мандатного контроля доступа реализован в ОС и СУБД, предназначенных для работы с информацией высокого уровня конфиденциальности, как то:

– программные продукты Научно-технического предприятия «Криптософт»: «QP ОС является многопользовательской операционной системой. Пользователи в системе обладают набором полномочий, заданных администратором системы. Исходя из полномочий пользователя, система определяет права доступа пользователя к объектам на основе штатных средств: дискреционного контроля доступа, мандатного контроля доступа и мандатного контроля доверия» [9]. «СУБД QP DB поддерживает разграничение доступа к данным как с применением классической модели мандатного разграничения доступа, так и с применением многоэкземплярной модели мандатного разграничения доступа как на уровне атрибутов, так и на уровне строк таблиц» [10];

– программные продукты «НПО Русбитех» [11]: в ОС специального назначения Astra Linux Special Edition «Механизмы мандатного управления доступом реализованы в ядре ОС. При этом принятие решения о запрете или разрешении доступа принимается на основе типа операции, мандатного контекста безопасности субъекта и мандатной метки объекта». Правила применения соответствуют приведенным выше правилам [3]. В ОС реализовано мандатное разграничение на уровне ее объектов, в первую очередь файлов и каталогов, в «качестве защищенной СУБД в составе ОС используется СУБД PostgreSQL версии 9.6, доработанная в

соответствии с требованием интеграции с ОС в части мандатного управления доступом к информации и содержащая реализацию ДП-модели управления доступом и информационными потоками. Данная ДП-модель описывает все аспекты дискреционного, ролевого и мандатного управления доступом»;

– система принудительного контроля доступа SELinux для ОС семейства Linux [12]. Первая версия SELinux разработана National Information Assurance Research Laboratory, подразделением Агенства национальной безопасности США (АНБ), в сотрудничестве с Secure Computing Corporation. В SELinux права доступа определяются самой системой при помощи специально определенных политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux. Иными словами, через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации.

Механизм мандатного контроля целостности реализован в ряде операционных систем. Так, в ОС семейства Windows, начиная с Windows Vista [13, 14], внедрена новая функция безопасности Mandatory Integrity Control, MIC (обязательный контроль целостности), которая добавляет управление доступом с помощью уровней целостности. Уровень целостности представляет собой уровень надежности субъекта или объекта доступа. Цель этого механизма заключается в использовании политик управления целостностью и уровнями целостности задействованных субъектов и объектов для ограничения доступа процессам, которые считаются потенциально менее надежными, по сравнению с доверенными процессами, работающими под той же учетной записью пользователя.

В Windows определены следующие пять уровней целостности (в порядке возрастания): недоверенный, низкий, средний, высокий, системный. Для объектов Windows по умолчанию заданы мандатные политики целостности No-Write-Up и No-Read-Up, т.е. процесс не может взаимодействовать с другим процессом, имеющим более высокий уровень целостности. Тем самым он не может выполнять такие функции, как внедрение динамически загружаемых библиотек в процесс высшего уровня целостности, используя функцию создания удаленного потока, отправить данные в другой процесс, используя функцию записи памяти процесса или открыть для записи или чтения файл с более высоким уровнем целостности.

Приведенные правила несколько отличаются от классической модели Биба: нет запрета на обращение к объектам более низкого уровня целостности как для чтения, так и для записи, также присутствует запрет на чтение вверх. Таким образом, в данной реализации запрещены все обращения вверх и разрешены все обращения вниз.

В ОС Astra Linux Special Edition [11] используется решетка уровней целостности от 0 до 256, причем эти уровни представляют собой неиерархические категории, т.е. у конкретного объекта метка целостности представляет собой битовую маску, например, 0b01010101. При этом определены следующие правила сравнения меток целостности: метки пользователя iL0 и объекта iL1 равны, если их численные значения совпадают, а iL0 < iL1, если все биты набора iL0 являются подмножеством набора iL1. Тогда операция записи разрешена, если iL0 >= iL1, а операции чтения и исполнение разрешены для любого соотношения iL0 и iL1.

Отметим, что мандатный контроль целостности в случаях Windows и Astra Linux применяется к разным взаимодействующим объектам: в случае Astra Linux это взаимодействие пользователя с файлами и каталогами, а в случае Windows регламентируется взаимодействие процессов разного уровня целостности.

Представим описанные выше политики мандатного контроля целостности в виде таблицы ниже, имея в виду, что все рассматриваемые действия разрешены по правилам дискреционного разграничения («Да» означает, что действие разрешено, «Нет», что запрещено), причем при равных значениях уровней целостности чтение и запись разрешены.

Из приведенных в таблице данных следует, что разработчики политик безопасности реаль-

Наименование	Чтение вверх (Read Up)	Запись вверх (Write-Up)	Чтение вниз (Read-Down)	Запись вниз (Write-Down)
Модель Биба	Да	Нет	Нет	Да
Windows	Нет	Нет	Да	Да
Astra Linux SE	Да	Нет	Да	Да

ных ОС формируют их, исходя из требуемого функционала в части мандатного контроля целостности, при этом полного консенсуса для исполнения правил «чтение вверх» и «чтение вниз» не существует.

2. Реализация мандатного контроля в информационных системах

Из приведенного обзора видно, что мандатный контроль доступа и целостности обеспечивают дополнительные возможности при реализации деловой логики АИС. В данном разделе будут рассмотрены предложения по их практическому использованию.

2.1. Мандатный контроль доступа

Остановимся на некоторых особенностях классических алгоритмов работы мандатного контроля доступа:

– жесткая связь с сеансом работы пользователя в ОС. Это означает, что АИС получает от ОС мандатный профиль сеанса и присваивает его данные всем информационным объектам, создаваемым пользователем. При этом мандатный профиль конкретного сеанса работы определяется самим пользователем при входе в ОС, профиль выбирается из набора, являющегося одним из свойств учетной записи пользователя, задаваемых администратором безопасности;

– при выдаче пользователю для просмотра или редактирования объекта решение о возможности выполнения этого действия принимается путем сравнения мандатного профиля объекта и сеанса пользователя по правилам [3], описанным выше;

– изменение мандатного профиля информационного объекта логикой работы АИС не предусматривается.

Перечисленные особенности накладывают существенные ограничения на реализацию деловой логики АИС, что зачастую приводит к отказу от использования мандатного контроля. Одной из значимых проблем является запрет сохранения отредактированной информации с меньшим уровнем конфиденциальности, чем уровень конфиденциальности работающего пользователя, поскольку при приведенных выше ограничениях потребуется поднять уровень конфиденциальности данных, чтобы не допустить информационный поток «сверху вниз».

Предлагается следующая модификация правил мандатного разграничения доступа.

1. Иерархические категории вновь создаваемых информационных объектов могут назначаться пользователем самостоятельно не выше соответствующей категории, заданной для настоящего сеанса работы.

2. Неиерархические категории новых объектов также присваиваются пользователем самостоятельно из набора категорий настоящего сеанса.

3. Право на чтение информационных объектов (при наличии этого права по дискреционным правилам) определяется по правилам [3], т.е. можно читать те объекты, для которых все иерархические категории не выше соответствующих категорий сеанса пользователя. При этом в случае, если в профиле объекта присутствует значение иерархической категории, которая отсутствует в профиле сеанса, чтение запрещается. Для неиерархических категорий требуется наличие всех категорий профиля объекта в профиле сеанса.

4. Модифицировать разрешается все информационные объекты, доступные для чтения по мандатным правам и для редактирования по дискреционным.

5. При сохранении объекта после редактирования его мандатный профиль не изменяется. При этом сами пользователи отвечают за то, чтобы не допустить информационные потоки «сверху» «вниз», т.е. внесение в редактируемые данные информации повышенного уровня конфиденциальности.

6. Изменение мандатного профиля объекта – это отдельное действие, доступное крайне ограниченному кругу пользователей.

Рассмотрим, какие появляются дополнительные возможности при реализации мандатного контроля в АИС.

Согласно п.1 и п.2 появляется возможность произвольного задания мандатного профиля объекта пользователем, что полностью соответствует логике работы с бумажными документами, когда степень конфиденциальности создаваемого документа определяется его автором.

Рассмотрим варианты реализации данных предложений на примере СЭД.

– Пусть в ОС определены иерархические категории Уровень конфиденциальности с значениями «Не для печати», «Конфиденциально» и «Строго конфиденциально», а также Должность с значениями «Все сотрудники», «Заместители директора» и «Директор» Тогда если пользователь работает с мандатным профилем {«Строго конфиденциально» + «Заместитель директора»}, он может присвоить создаваемому объекту мандатный профиль {«Не для печати» + «Все сотрудники»}, но не может {«Строго конфиденциально» + «Директор»}.

– Пусть в ОС определены неиерархические категории, соответствующие подразделениям: «Бухгалтерия», «Отдел кадров», «Плановый отдел», «Канцелярия». Тогда если пользователь работает с мандатным профилем {«Бухгалтерия» + «Отдел кадров» + «Плановый отдел»}, он может присвоить новому объекту профиль {«Бухгалтерия» + «Плановый отдел»}, но не может присвоить категорию «Канцелярия».

Согласно п. 3 обеспечивается возможность одновременного просмотра пользователем объектов разного уровня конфиденциальности, что позволяет видеть всю совокупность необходимых в данный момент данных одновременно и позволяет разбить один информационный объект на несколько разных объектов с разными мандатными профилями. В частности, для СЭД, работающих с электронными документами и их регистрационными карточками, в большинстве случаев требуется разный уровень конфиденциальности для карточки и содержательной части. Это требование обусловлено действующими инструкциями по делопроизводству, позволяющими хранить бумажные регистрационные карточки в открытом доступе при условии, что в них не вносится информация высокого уровня конфиденциальности. При разработке СЭД требуется учитывать, что указанные части одного информационного объекта могут иметь разный уровень конфиденциальности и обрабатываться по разным правилам. Эту задачу можно несколько упростить, сделав карточки и сами документы разными, но связанными информационными объектами, и предусмотрев удобный интерфейсный способ одновременного просмотра этих объектов. При этом необходимо учесть, что даже в случае работы пользователя в сеансе с высоким уровнем конфиденциальности он должен иметь возможность редактирования карточки без повышения ее уровня.

Согласно п. 4 и 5 появляется возможность редактирования объектов без обязательного повышения уровня конфиденциальности и других изменений мандатного профиля редактируемых данных.

Согласно пункту 6 появляется возможность контроля и исправления мандатных профилей объектов по мере необходимости. Данная возможность требуется и согласно [3]. Это право может рассматриваться как отдельная привилегия, присваиваемая администраторам безопасности и, возможно, руководителям в части модификации мандатных профилей информационных объектов своего подразделения.

В конкретной реализации АИС может быть принято решение о выделении некоторых иерархических категорий, для которых изменение значений полностью запрещено, в первую очередь это может касаться уровня конфиденциальности информационного объекта.

2.2. Мандатный контроль целостности

Предлагаются следующие правила применения мандатного контроля целостности в АИС.

1. Мандатный контроль целостности применяется только для ограничений на выполнение пользовательских операций с объектами.

2. Метки целостности информационных объектов назначаются автоматически при осуществлении операций в системе, и зависят от состояния объекта.

3. Метки целостности субъектов могут наследоваться.

4. Метки целостности неиерархические, они не зависят друг от друга. Операция считается

разрешенной, если все метки объекта содержатся в метках субъекта.

5. Метки целостности субъектов могут изменять только выделенные пользователи, например, администраторы безопасности.

6. Пользователь может самостоятельно изменять метку целостности сеанса работы в пределах набора этих меток, установленных администратором безопасности для его учетной записи.

Правило 1 справедливо для АИС, использующих и мандатный контроль доступа, и мандатный контроль целостности, и служит для четкого определения сферы применения каждого механизма. Мандатные метки доступа назначаются объекту при создании и, как правило, не меняются. Изменение может производиться только выделенными субъектами и только по регламенту. Мандатные метки целостности назначаются в процессе жизненного цикла обработки объекта автоматически.

Правило 2 регулирует автоматическое назначение мандатных меток целостности в зависимости от состояния объекта. Данное правило позволяет, например, организовать запрет редактирования документа, обрабатываемого СЭД, при помещении его в архив. Преимущество такого решения по сравнению с механизмом изменения дискреционных прав состоит в неизменности списка доступа к документу, что позволит продолжать работу с ним в случае снятия запрета редактирования (например, возврата документа из архива), а, тем самым, увеличит быстродействие подсистемы управления доступом.

Правило 3 определяет алгоритм назначения мандатных меток целостности в случае членства пользователя в группах и при его назначении на роль. В отличие от мандатных меток доступа метки целостности могут наследоваться субъектами (учетными записями пользователей от ролей и групп пользователей). При этом итоговая метка целостности пользователя представляет собой сумму меток группы и его собственной учетной записи.

Правило 4 определяет способ сравнения мандатных меток контроля целостности. Независимость меток необходима для упрощения применения и реализации механизма мандатного контроля целостности.

Правило 5 определяет порядок изменения мандатных меток целостности для субъектов.

Правило 6 предусматривает возможность изменения пользовательских привилегий в процессе работы, что служит дополнительной защитой от непреднамеренных ошибочных действий. Так, администратор может работать с правами обычного пользователя, поднимая уровень своих полномочий только для выполнения действий по настройке АИС. Предлагаемая логика позволяет упростить процесс ведения БД пользователей, т.к. в норме администраторам рекомендуется иметь различные учетные записи для выполнения административных действий и для обычной работы.

В качестве примера использования предложенных правил рассмотрим следующий алгоритм реализации мандатного контроля целостности в системе электронного документооборота. Деловая логика таких систем предусматривает запрет редактирования электронных документов в целом ряде случаев. Это относится, в первую очередь, к входящим документам, поступившим из внешних организаций, исходящим документам, отправленным адресатам, документам, переданным на хранение в архив или утвержденным руководителям. При этом с точки зрения дискреционных правил разграничения доступа документы могут редактироваться достаточно широким кругом пользователей от их создателя до руководства подразделения или организации.

Запрет в этом случае реализуется путем задания каждой категории учетных записей и каждой категории документов системы метки целостности в виде битовых масок, причем редактировать рассматриваемый объект разрешено только в том случае, когда все биты метки объекта входят в биты метки субъекта, т.е. в терминах [11] уровень целостности субъекта равен или превосходит уровень целостности объекта.

В рассмотренных случаях признак запрета редактирования должен устанавливаться автоматически после совершения определенных действий в СЭД (сдача в архив, регистрация входящего документа и т.д.) Снятие такого признака должно быть следствием четко определенных действий,

например, отмена утверждения документа для продолжения работы с ним.

С точки зрения деловой логики СЭД описанные правила удобно использовать для обеспечения неизменности целого ряда документов.

Заключение

Широкое внедрение цифровых технологий во все отрасли народного хозяйства, образование, государственное управление, которое часто называют их цифровизацией, невозможно без надежного обеспечения безопасности обрабатываемой информации, причем системы безопасности должны быть максимально гибкими для учета особенностей деловой логики автоматизируемых предприятий и организаций. В связи с этим алгоритмы работы таких систем постоянно совершенствуются, это относится и к подсистемам управления доступом пользователей к информационным объектам. Рассмотренные в настоящей работе алгоритмы мандатного контроля доступа и целостности предоставляют новые возможности при разработке таких подсистем и могут использоваться в АИС различного назначения.

Разграничение доступа по уровням конфиденциальности информации и по подразделениям организации дает возможность более точно учитывать особенности обрабатываемых данных, используя при этом свойства учетной записи работающего пользователя. Запрет редактирования отдельных категорий информационных объектов делает работу информационных систем более логичной, разгружая при этом подсистемы дискреционного контроля доступа.

Рассмотренные способы разграничения доступа уже сейчас востребованы IT отраслью, а в будущем их применение будет расширяться.

Литература

1. Bell D.E., La Padula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. – Bedford, Mass.: MITRE Corp., 1976. – MTR-2997 Rev. 1.
2. Biba, K. J. Integrity Considerations for Secure Computer Systems, MTR-3153, The Mitre Corporation, June 1975.
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ ФСТЭК. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. http://www.fstec.ru/_docs/doc_3_3_003.doc.
4. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.
5. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18 февраля 2013 г. N 21.
6. Мандатная модель управления доступом (MAC): обзор и применение в прикладных системах. https://habr.com/ru/company/avanpost/blog/482060/, доступно 05.02.2020.
7. Акимова Г.П., Даниленко А.Ю., Пашкина Е.В., Пашкин М.А., Подрабинович А.А., Соловьев А.В., Туманова И.В. Подход к автоматизации деловых процессов научной организации. Часть 2. Обеспечение информационной безопасности // Системы высокой доступности. 2019. Т. 15. № 2. С. 20–31. DOI 10.18127/j20729472-201902-02.
8. Даниленко А.Ю. Безопасность систем электронного документооборота: Технология защиты электронных документов. Изд. 2-е, дополненное. / М: ЛЕНАНД. 2020г. 240 стр. (Основы защиты информации. № 13). (С) ЛЕНАНД, 2015, 2019.
9. Операционная система QP ОС. https://cryptosoft.ru/qpos.html.
10. Система управления базами данных QP DB. https://cryptosoft.ru/PO1.html.
11. Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1. РУСБ. 10015-01 97 01-1. 2018 год.
12. SELinux Documentation. https://www.nsa.gov/what-we-do/research/selinux/documentation/
13. Steve Riley on Security. Mandatory integrity control in Windows Vista. https://docs.microsoft.com/ru-ru/archive/blogs/steriley/mandatory-integrity-control-in-windows-vista.
14. Matthew Conover. Analysis of the Windows Vista Security Model. https://pdfs.semanticscholar.org/08b8/e93db85403bec019ff091048c4342a72d301.pdf.

Акимова Галина Павловна. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Ведущий научный сотрудник. Кандидат технических наук. Количество печатных работ: более 70. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Ведущий научный сотрудник. Кандидат физико-математических наук. Количество печатных работ: более 40 (в т.ч. 1 монография, 2 издания). Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru

Пашкина Елена Владимировна. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Ведущий программист. Количество печатных работ: 15. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Пашкин Матвей Александрович. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Научный сотрудник. Количество печатных работ: 20. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив.E-mail: pashkin@isa.ru

Подрабинович Андрей Александрович. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Ведущий программист. Количество печатных работ: 10. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации в документооборотных системах. E-mail: podrabinovich@isa.ru

Туманова Ирина Владимировна. Федеральный исследовательский центр «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН), г. Москва, пр-т 60-летия Октября, 9. Ведущий программист. Количество печатных работ: 7. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: tumanova-irin@mail.ru

Mandatory Control in Automated Information Systems

G. P. Akimova, A. Yu. Danilenko, E. V. Pashkina, M. A. Pashkin, A. A. Podrabinovich, I. V. Tumanova

Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The article discusses access control and integrity control using mandatory algorithms. Currently, these approaches to ensuring information security are not widely used in the development of automated information systems due to restrictions on their implementation. The authors proposed a change in these restrictions, replacing them with a number of rules that allow more accurately take into account the business logic of operating organizations. This approach allows to significantly expand the application of mandatory control in all types of information systems.

Keywords: information security, automated information systems, mandatory access control, mandatory integrity control.

DOI 10.14357/20718632200301

References

1. Bell D.E., La Padula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. - Bedford, Mass.: MITER Corp., 1976. - MTR-2997 Rev. 1.
2. Biba, K. J. Integrity Considerations for Secure Computer Systems, MTR-3153, The Miter Corporation, June 1975.
3. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii. Rukovodyashchiy dokument FSTEK. [Computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information. FSTEC guidance document]. http://www.fstec.ru/_docs/doc_3_3_003.doc.
4. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. [On approval of requirements for the protection of information not constituting state secrets contained in state information systems. Order of the FSTEC of Russia].
5. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti per-

sonal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. [On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems. Order of the FSTEC of Russia].
6. Mandatnaya model' upravleniya dostupom (MAC): obzor i primeneniye v prikladnykh sistemakh. [Mandatary Access Control Model (MAC): overview and application in application systems]. https://habr.com/en/company/avanpost/blog/482060/, available 05.02.2020.
7. Akimova G.P., Danilenko A.Yu., Pashkina E.V., Pashkin M.A., Podrabinovich A.A., Soloviev A.V., Tumanova I.V. 2019. Podkhod k avtomatizatsii delovykh protsessov nauchnoy organizatsii. Chast' 2. Obespecheniye informatsionnoy bezopasnosti. [An approach to the automation of business processes of a scientific organization. Part 2. Ensuring information security]. Sistemy vysokoy dostupnosti. [High Availability Systems]. 2: 20-31. DOI 10.18127 / j20729472-201902-02.
8. Danilenko A.Yu. 2020. Bezopasnost' sistem elektronnogo dokumentooborota: Tekhnologiya zashchity elektronnykh dokumentov. Izd. 2-ye, dopolnennoye. [Security of electronic document management systems: Technology for the protection of electronic documents. Ed. 2nd, supplemented]. Moscow: LENAND. 240 p.
9. Operatsionnaya sistema QP OS. [The operating system QP OS]. https://cryptosoft.ru/qpos.html.
10. Sistema upravleniya bazami dannykh QP DB. [Database Management System QP DB]. https://cryptosoft.ru/PO1.html.
11. Operatsionnaya sistema spetsial'nogo naznacheniya «Astra Linux Special Edition». Rukovodstvo po KSZ. Chast' 1. [The special-purpose operating system "Astra Linux Special Edition". KSZ Guide. Part 1]. Moscow: RUSB. 10015-01 97 01-1. 2018.
12. SELinux Documentation. https://www.nsa.gov/what-we-do/research/selinux/documentation/
13. Steve Riley on Security. Mandatory integrity control in Windows Vista. https://docs.microsoft.com/en-us/archive/blogs/steriley/mandatory-integrity-control-in-windows-vista.
14. Matthew Conover. Analysis of the Windows Vista Security Model. https://pdfs.semanticscholar.org/08b8/e93db85403bec019ff091048c4342a72d301.pdf.

Akimova G. P. PhD, Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: akimova@isa.ru

Danilenko A. Yu. PhD, Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: danilenko@isa.ru

Pashkina E. V. Lead programmer. Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: pashkina@isa.ru

Pashkin M. A. Researcher. Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: pashkin@isa.ru

Podrabinovich A. A. Lead programmer. Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: podrabinovich@isa.ru

Tumanova I. V. Lead programmer. Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, e-mail: tumanova-irin@mail.ru