УДК 681.3

Шорошев В.В.

ПРАВИЛА ПОЛИТИКИ УПРАВЛЕНИЯ ДОСТУПОМ К РЕСУРСАМ ЛОКАЛЬНЫХ СЕТЕЙ INTRANET, МЕХАНИЗМЫ ИХ РЕАЛИЗАЦИИ

Политика безопасности ресурсов любой компьютерной системы обеспечивается, прежде всего, так называемыми "услугами безопасности", среди которых приоритетное место занимают и модели управления доступом, а также "механизмы" их реализации. Они являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа "субъектов" к защищаемым информационным и техническим ресурсам – "объектам". В качестве "субъектов" в простейшем случае понимается пользователь. На практике же наличие механизмов управления доступом необходимо, даже если в системе может находиться только один ее пользователь. Дело в том, что в системе обязательно должен быть еще один пользователь с правами "администратора безопасности", который настраивает параметры системы защиты и права доступа к ресурсам защищаемого объекта.

Правила политики управления доступом и механизмы их реализации рассмотрим в такой постановке задачи [3,4,7,8,9,10,12,14].

Во-первых, основное внимание сосредоточим на управлении доступом к ресурсам сетей Intranet, т.е. корпоративных локальных сетей, имеющих постоянное или временное соединение с информационной супермагистралью Internet.

Во-вторых, политика безопасности сетей Intranet, как и любой компьютерной системы, всегда реализуется комплексом нормативно-правовых, программно-технических и организационных "услуг безопасности", среди которых приоритетное место занимают и услуги безопасности "механизмов" управления доступом.

Используя фундаментальные теоретические проработки "механизмов" управления доступом к ресурсам компьютерных систем по результатам работ Российской Федерации [1,2,11,12,13], рассмотрим существующие классические модели управления доступом (абстрактные, канонические, дискреционные, мандатные, с виртуальными каналами взаимодействия и т.п.), а также основные механизмы реализации их "услуг безопасности". Вначале рассмотрим абстрактные модели управления доступом (модели защиты).

Модель Биба. Одной из первых абстрактных моделей была опубликованная в 1977 модель Биба (Biba). Согласно этой модели все субъекты и объекты предварительно разделяются по нескольким уровням доступа. Затем на их взаимодействия накладываются следующие ограничения: субъект не может вызывать на исполнение субъекты с более низким уровнем доступа; субъект не может модифицировать объекты с более высоким уровнем доступа.

Модель Гогена-Мезигера. Модель Гогена-Мезигера (Goguen-Meseguer), представленная ими в 1982 году, основана на теории автоматов. Согласно этой модели система может при каждом действии переходить из одного разрешенного состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы — домены.

Переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано, какие операции может выполнять субъект, например, из домена C над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская модель. Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, основана на взаимодействии субъектов и потоков информации. Так как и в предыдущей модели, здесь используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной

модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Модель Кларка-Вильсона. Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. В данной модели впервые исследована защищенность третьей стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор. Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены субъекта в момент между его идентификациями. Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

Дискреционная (матричная) модель. Рассмотрим так называемую матричную модель защиты (ее еще называют дискреционной моделью), получившую на сегодняшний день наибольшее распространение на практике. В терминах матричной модели состояние системы защиты описывается тройкой матричных множеств *(S, O, M)*, где:

S — множество субъектов, являющихся активными структурными элементами модели;

O — множество объектов доступа, являющихся пассивными защищаемыми элементами модели. Каждый объект однозначно идентифицируется с помощью имени объекта;

M -- матрица доступа. Значение элемента матрицы *M {S,O}* определяет права доступа субъекта *S к* объекту *O.*

Права доступа регламентируют способы обращения субъекта *S* к различным типам объектов доступа. В частности, права доступа субъектов к файловым объектам обычно определяют как чтение *(R)*, запись *(W)* и выполнение *(E)*.

Основу реализации услуг безопасности по управлению доступом составляет анализ строки матрицы доступа при обращении субъекта к объекту. При этом проверяется строка матрицы, соответствующая объекту, и анализируется, есть ли в ней разрешенные права доступа для субъекта или нет. На основе этого принимается решение о предоставлении доступа.

При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, матричным моделям присущи серьезные недостатки. Основной из них- это излишне детализированный уровень описания отношений субъектов и объектов. Из-за этого усложняется процедура администрирования системы защиты. Как следствие, усложнение администрирования может приводить к возникновению ошибок.

Многоуровневые (мандатные) модели. С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Д. Деннинг. Многоуровневые модели предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или мандатов, назначаемых субъектам и объектам доступа.

Так, для субъекта доступа метки, например, могут определяться в соответствии с уровнем допуска лица к информации, а для объекта доступа (собственно данные) -- признаками конфиденциальности информации. Признаки конфиденциальности фиксируются в метке объекта. В связи с использованием терминов "мандат", "метка", "полномочия" многоуровневую защиту часто называют соответственно либо мандатной защитой, либо защитой с метками конфиденциальности, либо полномочной защитой.

Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий

конфиденциальности. Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например: конфиденциально, секретно, для служебного пользования, несекретно и т.п.

Основу реализации услуг безопасности по управлению доступом составляют:

1. Формальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрошен доступ.

2. Принятие решений о предоставлении доступа на основе некоторых правил, основу которых составляет противодействие снижению уровня конфиденциальности защищаемой информации.

Таким образом, - многоуровневая модель предупреждает возможность преднамеренного или случайного снижения уровня конфиденциальности защищаемой информации за счет ее утечки (умышленного переноса). Эта модель препятствует переходу информации из объектов с высоким уровнем конфиденциальности и узким набором категорий доступа в объекты с меньшим уровнем конфиденциальности и более широким набором категорий доступа.

Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа. Причем, так как отдельно взятые категории одного уровня равнозначны, то, чтобы их разграничить наряду с многоуровневой (мандатной) моделью, требуется применение матричной модели.

С помощью многоуровневых моделей возможно существенное упрощение задачи администрирования (настройки). Причем это касается как исходной настройки разграничительной политики доступа (не требуется столь высокого уровня детализации задания отношения субъект-объект), так и последующего включения в схему администрирования новых объектов и субъектов доступа.

Выбор дискреционной и мандатной моделей доступа. Следуя формализованным требованиям к системе защиты информации, основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является дискреционный механизм управления доступом, а секретных сведений – мандатный механизм управления доступом.

Дискреционная модель управления доступом. Следуя формализованным требованиям к системе защиты информации, основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является дискреционный механизм управления доступом. При этом к нему предъявляются следующие требования:

1. Система защиты должна контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.);

2. Для каждой пары (субъект — объект) в средстве вычислительной техники (СВТ) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту);

3. Система защиты должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа;

4. Контроль доступа должен быть применим к каждому объекту и каждому субъекту;

5. Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил или прав разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов;

6. Право изменять ПРД должно предоставляться выделенным субъектам (администратору или службе безопасности и т.д.);

7. Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Мандатная модель управления доступом. Основу реализации разграничительной политики доступа к ресурсам при защите секретной информации является требование к реализации, помимо дискреционного, обязательно и мандатного механизма управления доступом. Требования к мандатному механизму состоят в следующем:

1. Каждому субъекту и объекту доступа должны сопоставляться классификационные метки, отражающие их место в соответствующей иерархии (метки конфиденциальности). Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости; категории секретности; необходимый или максимальный уровни безопасности; допустимый, заданный или минимальный уровни ограничений видов информационной деятельности и т. п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа;

2. Система защиты при вводе новых данных в систему должна запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта ему должны назначаться классификационные метки. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри системы защиты);

3. Система защиты должна 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. При этом иерархические категории в классификационном уровне субъекта должны включать 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. При этом все иерархические категории в классификационном уровне субъекта должны включаться в иерархические категории в классификационном уровне объекта;

4. Реализация мандатных ПРД должна предусматривать возможность сопровождения, изменения классификационных уровней субъектов и объектов специально выделенными субъектами;

5. В СВТ должен быть реализован ***диспетчер доступа***, т.е. средство, которое осуществляет, во-первых, перехват всех обращений субъектов к объектам, а во-вторых, разграничивает доступ в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его дискреционными и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Каноническая модель управления доступом. В данном разделе обоснуем основополагающие принципы решения задачи управления доступом к ресурсам, в предположении, что пользователь не является "владельцем" информации.

Понятия "владелец" и "собственник" информации. Принципиальным моментом при исследовании проблем управления доступом к ресурсам является трактовка понятия "владельца" информации (в терминологии, применяемой при реализации механизмов управления доступом в ОС) или соответственно "собственника" информации (как увидим далее, это не одно и то же). Сформулируем эти понятия, исходя из формализованных требований к механизмам защиты [1,2,12], а также из принципов реализации встроенной защиты в современных универсальных ОС. При этом будем учитывать, что "владелец"

файлового объекта во встроенных в ОС механизмах защиты может устанавливать и изменять атрибуты доступа, т.е. назначать и распространять ПРД.

На сегодняшний день в качестве "владельца" информации рассматривается либо пользователь, либо некое ответственное лицо. В качестве последнего, как правило, выступает сотрудник подразделения безопасности, в частности, администратор безопасности. Здесь же отметим, что в существующих ОС пользователь сам может устанавливать атрибуты на создаваемые им файловые объекты и не во всех случаях данные действия пользователя могут осуществляться в рамках задаваемых администратором разграничений прав доступа к ресурсам.

Таким образом, в рамках существующих ОС "владелец" объекта файловой системы - это лицо, которое может устанавливать права доступа (атрибуты) к данному файловому объекту. В общем случае это может быть либо администратор, либо пользователь, создающий файловый объект. Однако права "владельца", в конечном счете, определяются тем, кто является собственником информации, т.к. только "собственник" информации может принимать решение ее передачи другим лицам. Естественно, что когда речь идет о домашнем компьютере, то "собственником" и "владельцем" является непосредственный хозяин компьютера, обрабатывающий на нем собственную информацию.

Другое дело -- применение вычислительных средств (соответственно средств защиты) на предприятии. Использование защищаемого компьютера на предприятии, как правило, связано с защитой служебной информации, конфиденциальных данных и т.д. Но эта информация уже не является собственностью пользователя, следовательно, не пользователь должен являться ее конечным "владельцем". При этом также необходимо учитывать, что по статистике большинство хищений информации на предприятии (умышленно или нет) осуществляется непосредственно сотрудниками, в частности, пользователями защищаемых компьютеров. Естественно, то же (но в большей мере) относится к защите секретной информации, собственником которой является государство.

Более того, владельцем служебной информации является предприятие. Что касается конфиденциальной информации, то здесь все зависит от ее типа. Иными словами, в связи с этим большинство приложений систем защиты уже фактически связано именно с защитой "данных", собственником которых пользователь не является.

На практике существует некоторое противоречие в определении дискреционного управления доступом и требований, формулируемых к его реализации. Так, определение дискреционного управления доступом предполагает: "Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту".

Другими словами, "владельцем" файлового объекта здесь является непосредственно пользователь. Именно данная концепция принимается в качестве основы создания разграничительной политики доступа к ресурсам в современных ОС, прежде всего, в ОС семейства Windows (говоря о разграничении доступа к файловым объектам для ОС Windows, мы подразумеваем файловую систему NTFS).

Вместе с тем, говоря о требованиях к системе защиты, предназначенной для обработки конфиденциальной информации, то обязательными услугами безопасности должны быть:

- контроль доступа должен быть применим к каждому объекту и к каждому субъекту (индивиду или группе равноправных индивидов);
- механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил или прав разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов;
- право изменять ПРД должно предоставляться выделенным субъектам (администратору безопасности, администрации и т.д.);

- должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ. Другими словами, рассмотренными требованиями к дискреционному управлению доступом регламентируется, что все права по назначению и изменению ПРД предоставляются не субъектам (пользователям), а выделенному субъекту — администратору безопасности. При этом должны быть предусмотрены средства, ограничивающие распространение прав на доступ, т.е. препятствующие передаче прав одним субъектом другому. Из данных требований вытекает, что в качестве "владельца" ресурса должен рассматриваться администратор безопасности, т.к. "владелец" имеет возможность назначить, изменить и распространить права на доступ.

Видим, что здесь вступают в противоречие концептуальные подходы к определению "владельца" информации, а как следствие и подходы к построению разграничительной политики доступа к ресурсам. В одном случае, если "владельцем" информации считать пользователя, то естественным будет предоставить ему возможность передачи прав доступа к своим ресурсам ("владельцем" которых он является) другим пользователям. В другом случае, если "владельцем" информации пользователь не является (что чаще всего), то все права по назначению и распространению (переназначению) прав доступа должны принадлежать выделенным субъектам - ответственным лицам "владельца" информации, например, администратору безопасности. В общем случае правомерен именно второй подход.

Поэтому, говоря о дискреционном управлении доступом, будем предполагать, что назначение и изменение ПРД в системе предоставляется выделенным субъектам — администраторам безопасности. При этом модели дискреционного доступа будем рассматривать именно в данных предположениях. Соответственно они будут отличаться от моделей, предусматривающих, что "владельцем" файлового объекта является пользователь.

Таким образом, можно сформулировать следующие правила политики управления доступом (ПУД) к ресурсам локальных сетей Intranet.

Правило ПУД-1: ***в основу разграничительной политики доступа к ресурсам локальной сети Intranet должен закладывается принцип: пользователь не является "собственником" обрабатываемой им информации, как следствие, не может рассматриваться ее "владельцем", т.е. не должен иметь право назначать и изменять правила разграничения доступа к объектам файловой системы. "Владельцем" объектов файловой системы должен рассматриваться администратор безопасности, являющийся ответственным лицом собственника, в частности, предприятия.***

Правило ПУД-2: ***в защищенной локальной сети Intranet реализуется политика защиты информации, "владельцем" которой априори не является ее пользователь, можно говорить только о защите "компьютерных данных", собственником которых пользователь не является, но может быть только их санкционированным и дисциплинированным владельцем, и только по правам доступа, предоставленным ему администратором безопасности.***

Выполнение рекомендаций этих правил дает возможность гармонизации требований нормативных документов Украины НД ТЗИ с выполнением норм права и рекомендаций Конвенции Совета Европы о киберпреступности в части международного сотрудничества в борьбе с преступлениями против конфиденциальности (несанкционированного ознакомления), целостности (несанкционированного изменения) и доступности (несанкционированного ограничения) компьютерных данных и систем.

В контексте данных правил исследуем более детально модели дискреционного и мандатного управления доступом к ресурсам. Рассмотрим, в чем состоит их принципиальное различие, сформулируем требования к соответствующим механизмам защиты и подходы к их реализации. Рассмотрим возможности реализации разрабатываемых моделей встроенными в операционные системы (ОС) механизмами защиты. Сразу отметим, что общим для всех моделей являет то, что администратор безопасности является "владельцем"

любого объекта файловой системы. То есть только он обладает правом назначить (изменить) атрибуты доступа.

Введем следующие обозначения. Пусть множества С = {С1,...,Ск} и О = {01,...,Ok} — соответственно линейно упорядоченные множества субъектов и объектов доступа. В качестве субъекта доступа Ci, i = l,...,k рассматривается как отдельный субъект, так и группа субъектов, обладающих одинаковыми правами доступа. Соответственно, в качестве объекта доступа 01, 1 = l,...,k может также рассматриваться как отдельный объект, так и группа объектов, характеризуемых одинаковыми правами доступа к ним.

Пусть S = {0, 1} — множество прав доступа, где "0" обозначает запрещение доступа субъекта к объекту, а "1" -- разрешение полного доступа. Тогда каноническую модель управления доступом можно представить матрицей доступа D, имеющей следующий вид:

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} \end{array}$$

Под канонической моделью управления доступом для линейно упорядоченных множеств субъектов (групп субъектов) и объектов (групп объектов) доступа понимается модель, описываемая матрицей доступа, элементы главной диагонали которой «1» разрешают полный доступ субъектов к объектам, остальные элементы «0» запрещают доступ субъектов к объектам.

Говоря о доступе, нами в этот атрибут не включается право назначения (изменения) "владельца" и право назначения (изменения) атрибутов доступа к объекту. Данные права выведены из схемы рассмотрения, поскольку они принадлежат администратору безопасности, который является "владельцем" любого объекта файловой системы. Данная модель управления доступом формально может быть описана следующим образом:

Dij = 1, если i = j, иначе Dij = 0.

Диспетчер доступа реализует механизм управления доступом корректно только в том случае, если его настройками (заданием учетных записей субъектов и объектов доступа и правил разграничения доступа) можно реализовать каноническую модель управления доступом.

Доказывается утверждение от обратного. Если каноническую модель управления доступом реализовать невозможно (т.е. присутствуют элементы "1" вне главной диагонали матрицы доступа), то в системе присутствует, по крайней мере, один объект, доступ к которому невозможно разграничить в полном объеме. При этом объект включается одновременно в несколько групп объектов, априори характеризуемых различными правами доступа к ним.

Правило ПУД-3. ***Любой механизм управления доступом должен позволять настройками диспетчера доступа сводить реализуемую им модель доступа к каноническому виду.***

Объекты доступа могут по своей сути существенно различаться: файловые объекты, ветви и ключи реестра ОС (для ОС Windows), принтеры, разделяемые сетевые ресурсы, устройства, ресурсы внешней сети (хосты) и т.д. К ним могут различаться типы доступа (например, файловые объекты и принтеры). Кроме того, на практике может быть ограничение на число ресурсов (например, принтеров в системе, к которым разграничивается доступ, может быть существенно меньше, чем субъектов доступа к ним).

Однако все это не противоречит общности сформулированного утверждения, требования которого должны выполняться механизмом управления доступом при соответствующих настройках системы и диспетчера доступа к объекту любого вида.

Например, диспетчер доступа к принтерам должен при включении в систему принтеров по числу субъектов доступа (в частности, пользователей) обеспечивать реализацию канонической модели управления доступом, где элементами матрицы доступа D будут "1" — доступ субъекту к принтеру разрешен, "0" — доступ субъекту к принтеру запрещен.

Правило ПУД-4. ***К каждому защищаемому ресурсу системы, требующему разграничения доступа, должен быть реализован диспетчер доступа, позволяющий соответствующими настройками сводить реализуемую им модель доступа к каноническому виду. Таким образом, механизм управления доступом к ресурсу реализован корректно только в том случае, если настройками диспетчера доступа реализуемая им модель доступа может быть приведена к каноническому виду.***

Рассмотренная выше каноническая модель управления доступом характеризуется полным разграничением доступа субъектов к объектам, при котором субъекты не имеют каналов взаимодействия, т.е. каналов обмена информацией. Однако такая возможность должна предусматриваться. Если в системе может находиться несколько субъектов (например, пользователей), то появляется задача предоставления субъектам возможности обмена информацией.

Правило ПУД-5. ***В задачу управления доступом в общем случае входит не только защита данных субъектов (в данном случае пользователей) от несанкционированного их прочтения другими субъектами, но и защита данных субъектов от возможности их искажения другими субъектами. Этим защита данных от несанкционированного доступа (НСД) принципиально отличается от защиты данных (управления доступом) с использованием средств криптографической защиты информации (КЗИ).***

Для иллюстрации сказанного, рассмотрим каноническую матрицу доступа D, реализуемую с использованием средств криптографической защиты,

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & Зп & \dots & Зп & Зп \\ Зп & Зп/Чт & \dots & Зп & Зп \\ \dots & \dots & \dots & \dots & \dots \\ Зп & Зп & \dots & Зп/Чт & Зп \\ Зп & Зп & \dots & Зп & Зп/Чт \end{bmatrix} \end{array}$$

где элемент "Зп" обозначает разрешение доступа с использованием операции "запись" (прочитать информацию пользователь может, но не имеет возможности ее преобразовать к читаемому виду, т.к. информация зашифрована, поэтому обозначаем подобное право доступа, как "Зп"), "Зп/Чт" — соответственно, операции "запись" и "чтение".

С учетом введенных выше понятий и определений данную матрицу доступа можно охарактеризовать, как каноническую матрицу доступа, расширенную дуплексными каналами взаимодействия между собою всех субъектов. При этом дуплексные каналы реализованы на основе активных симплексных каналов взаимодействия субъектов доступа с использованием операции "запись". Другими словами, это частный случай управления доступом, не обеспечивающий защиту данных от их несанкционированной модификации (удаления).

Модель управления доступом с взаимодействием субъектов доступа посредством выделенного канала. Особенностью данной модели является включение в систему *дополнительного объекта доступа* (группы объектов), используемого субъектами доступа в качестве *выделенного канала взаимодействия.* Отметим, что в качестве канала взаимодействия здесь должны использоваться дуплексные каналы. Причем в обе стороны взаимодействия должны быть реализованы как активный, так и пассивный симплексные каналы. Ниже представлена каноническая матрица доступа D.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \\ O_{k+1} \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & 0 & \dots & 0 & 0 \\ 0 & Зп/Чт & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & Зп/Чт & 0 \\ 0 & 0 & \dots & 0 & Зп/Чт \\ Зп/Чт & Зп/Чт & Зп/Чт & Зп/Чт & Зп/Чт \end{bmatrix} \end{array}$$

В представленной каноничекой матрице доступа D с выделенным каналом взаимодействия субъектов доступа полный доступ задается операциями "запись" и "чтение". Для организации выделенного канала взаимодействия в систему включен объект доступа Ок+1.

Недостатком данной модели, ограничивающим возможность ее практического использования, является доступность находящейся в канале информации одновременно всем субъектам доступа. Данный недостаток может преодолеваться созданием группы каналов взаимодействия (т.е. включением группы дополнительных объектов доступа, а в пределе - свой объект доступа для каждого канала взаимодействия субъектов доступа) с соответствующим разграничением к ним доступа субъектов. Однако это приводит к неэффективному использованию ресурсов защищаемого объекта.

Модели управления доступом с взаимодействием субъектов доступа посредством виртуальных каналов. Под *виртуальным каналом взаимодействия субъектов доступа пониматся канал взаимодействия, реализованный с использованием только существующих объектов доступа без включения в систему дополнительных объектов.* Естественно, что в соответствии с классификацией виртуальные каналы для рассматриваемых моделей должны быть дуплексными. При этом они должны строиться на основе реализации либо пассивных симплексных каналов, либо активных симплексных каналов, реализованных с использованием операции "добавления". Использование операции "запись" здесь недопустимо ввиду необходимости защиты информации субъектов от возможности ее модификации. Рассмотрим варианты моделей с виртуальным каналом взаимодействия.

Модель управления доступом с дуплексными виртуальными каналами взаимодействия на основе пассивных симплексных каналов. Рассмотрим матрицу доступа D для модели управления доступом с дуплексными виртуальными каналами взаимодействия на основе пассивных симплексных каналов.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & Чт & \dots & Чт & Чт \\ Чт & Зп/Чт & \dots & Чт & Чт \\ \dots & \dots & \dots & \dots & \dots \\ Чт & Чт & \dots & Зп/Чт & Чт \\ Чт & Чт & \dots & Чт & Зп/Чт \end{bmatrix} \end{array}$$

Модель управления доступом с дуплексными виртуальными каналами взаимодействия на основе пассивных симплексных каналов формально может быть описана следующим образом:

Dij = Зп/Чт, если i = j, иначе Dij = Чт.

К недостаткам данной модели можно отнести то, что она предотвращает лишь возможность несанкционированной модификации информации объектов, не разграничивая субъектам доступ к объектам "по чтению". Очевидно, что в таком виде виртуальный канал взаимодействия субъектов не применим. Он может использоваться лишь при введении дополнительных разграничений или условий для канала взаимодействия субъектов доступа.

Модель управления доступом с дуплексными виртуальными каналами взаимодействия на основе активных симплексных каналов. При организации канала взаимодействия субъектов доступа целесообразно рассматривать множество прав доступа

(Чт, Д}, используемое для реализации канала взаимодействия субъектов доступа. Здесь элемент "Д" обозначает добавление, то есть возможность пользователя добавить информацию в объект без возможности чтения объекта и без возможности модификации существующей в объекте информации. Право доступа "Зп/Чт" обозначает право пользователя на чтение и запись информации. Рассмотрим матрицу доступа D для модели управления доступом с дуплексными виртуальными каналами взаимодействия на основе активных симплексных каналов.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & Д & & Д & Д \\ Д & Зп/Чт & & Д & Д \\ \dots & \dots & \dots & \dots & \dots \\ Д & Д & \dots & Зп/Чт & Д \\ Д & Д & \dots & Д & Зп/Чт \end{bmatrix} \end{array}$$

Модель управления доступом формально может быть описана следующим образом:

Dij = Зп/Чт, если i = j, иначе Dij = Д.

Данная модель практически лишена недостатков, присущих ранее рассмотренным моделям. Здесь в полном объеме реализуется каноническая модель управления доступом. При этом обеспечивается возможность полноценного корректного взаимодействия субъектов доступа: каждый субъект доступа может взаимодействовать со всеми другими субъектами доступа системы без снижения уровня защищенности от НСД. Будем считать данную модель, наиболее приемлемой для использования в рассматриваемых приложениях. Именно эту модель будем считать канонической моделью управления доступом с взаимодействием субъектов. На основе этой модели сформулируем правило управления доступом.

Правило ПУД-6. ***Каноническая модель управления доступом с взаимодействием субъектов (групп субъектов) и объектов (групп объектов) регламентируется матрицей доступа, элементы главной диагонали которой "Зп/Чт" задают полный доступ субъектов к объектам, остальные элементы "Д" задают активные симплексные каналы взаимодействия с использованием операции "добавление".***

Различия и общность альтернативных моделей. Выше были рассмотрены различные модели управления доступом с виртуальными каналами взаимодействия. С учетом сказанного, можем сделать следующие выводы относительно различия и общности альтернативных моделей, а также сформулировать следующие правила политики управления доступом.

Правило ПУД-7. ***Модели управления доступом различаются реализуемым в них каналом (каналами) взаимодействия субъектов доступа. При этом канал взаимодействия может быть выделенным или виртуальным; пассивным или активным; симплексным либо дуплексным.***

Правило ПУД-8. ***Общим для рассматриваемых моделей управления доступом является то, что для корректной реализации канала взаимодействия субъектов доступа следует рассматривать не право доступа "Зп" — "запись", а право доступа "Д" – "добавление". Право "Д" предоставляет возможность пользователю добавить информацию в объект без возможности чтения объекта и без возможности модификации существующей в объекте информации при добавлении новой информации.***

Механизмы реализации дискреционной модели доступа. На сегодняшний день на практике наиболее широко используются модели дискреционного и мандатного механизмов управления доступом. Рассмотрим регламентацию (формализацию) услуг безопасности механизмом дискреционной модели.

Дискреционный механизм управления доступом регламентирует способ обработки запросов диспетчером доступа и основан на задании правил разграничения доступа в диспетчере некоторой матрицей доступа D. Он предполагает задание в качестве учетной

информации субъектов и объектов их идентификаторов (например, имя пользователя и имя файлового объекта), а в качестве правил разграничения доступа — матрицы доступа D.

При запросе доступа, поступающего в диспетчер доступа от субъекта, диспетчер из запроса получает идентификаторы субъекта и объекта. Затем он находит элемент матрицы доступа на основе учетных данных субъекта и объекта, осуществляет управление запросом доступа на основании выбранного элемента матрицы доступа.

С учетом того, что при управлении доступом диспетчером анализируется собственно матрица доступа, дискреционный механизм управления доступом является универсальным в том смысле, что им может быть реализована любая из рассмотренных выше моделей управления доступом, в том числе и модель полномочного управления.

Пример частной матрицы доступа D для модели управления доступом с дуплексными виртуальными каналами взаимодействия на основе активных симплексным каналов представлен ниже.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & \partial & \dots & 0 & \partial \\ \partial & Зп/Чт & \dots & \partial & \partial \\ \dots & \dots & \dots & \dots & \dots \\ \partial & Д & \dots & Зп/Чт & Д \\ 0 & 0 & \dots & Д & Зп/Чт \end{bmatrix} \end{array}$$

Механизмы реализации мандатной модели доступа. В отличие от дискреционного механизма управления доступом, с применением которого может быть реализована любая модель управления доступом (посредством задания правил разграничения доступа в диспетчере матрицей доступа), мандатный механизм реализует полномочные модели управления доступом.

Метки безопасности. Основой мандатного механизма является включение в схему управления доступом так называемых меток безопасности (иерархических, так как в системе реализуется иерархия полномочий). Эти метки призваны отражать полномочия субъектов и объектов. При этом разграничение прав доступа в диспетчере уже может задаваться не матрицей доступа, а правилами обработки меток, на основании которых диспетчер принимает решение о предоставлении запрашиваемого доступа к ресурсу. В качестве же учетной информации субъекта и объекта доступа является метка безопасности. Впервые разграничение доступа на основе задания и обработки меток безопасности было предложено Беллом и Ла-Падулой [12].

Метки безопасности являются элементами линейно упорядоченного множества M = {Ml,...,Mk} и задаются субъектам и объектам доступа. Метки безопасности назначаются субъектам и объектам (группам субъектов и объектов). Они служат для формализованного представления их уровня полномочий.

Будем считать, что чем выше полномочия субъекта и объекта (меньше их порядковый номер в линейно полномочно упорядоченных множествах субъектов и объектов — C = {C1,..., Ск} и O = {O1,..., Ok}), тем меньшее значение метки безопасности Mi, i = 1,...,k им присваивается, т.е.: Ml < M2 < M3<...<Mk.

Таким образом, в качестве учетной информации субъектов и объектов доступа, кроме их идентификаторов (имен), в диспетчере доступа каждому субъекту и объекту задаются метки безопасности из множества M.

Возможности мандатной модели доступа. Под мандатным механизмом управления доступом, реализующим канонические полномочные модели управления доступом, понимается способ обработки запросов диспетчером доступа, основанный на формальном сравнении меток безопасности субъектов и объектов доступа в соответствии с заданными правилами. Сформулируем это более подробно следующим правилом.

Правило ПУД-9. ***Основой мандатного механизма является реализация принудительного управления виртуальными каналами взаимодействия субъектов***

доступа. При этом основным требованием к принудительному управлению является обеспечение невозможности перенесения информации из объекта более высокого уровня конфиденциальности в объект с информацией более низкого уровня конфиденциальности.

Поэтому к механизмам управления доступом, реализующим принудительное управление виртуальными каналами взаимодействия субъектов доступа, накладываются дополнительные ограничения к корректности реализации.

На практике для дискреционного механизма управления доступом, как правило, используется модель произвольного управления виртуальными каналами взаимодействия субъектов доступа. Однако управление каналами может быть и принудительным — все зависит от реализуемой матрицы доступа. В этом случае мандатный и дискреционный механизмы различаются только способом задания разграничительной политики в диспетчере доступа и обработки запросов на доступ.

Правило ПУД-10. ***Мандатный механизм управления доступом позволяет корректно реализовать полномочные модели управления доступом при условии, что всем субъектам и объектам доступа сопоставлены метки безопасности. Метки безопасности должны устанавливаться на все объекты файловой системы (логические диски (тома), каталоги, подкаталоги, файлы), а также на все иные объекты доступа — на устройства ввода/вывода и отчуждаемые носители информации, виртуальные каналы связи и т.п. Если существует объект, который не включен в схему мандатного управления доступом, то этот объект может являться средством несанкционированного взаимодействия пользователей, имеющих различные метки безопасности.***

Для дискреционного механизма, реализующего принудительное управление виртуальными каналами, это соответственно означает необходимость задания разграничений для всех субъектов и объектов доступа. Доказательство данного утверждения очевидно. Нетрудно показать, что представленные правила реализуют разграничения доступа полностью адекватные соответствующим каноническим матрицам доступа D, отображающим полномочные модели управления доступом, в случае, если всем субъектам из множества С и объектам из множества О сопоставлены метки безопасности. При этом несопоставление метки безопасности какому-либо субъекту или объекту означает вычеркивание соответствующей строки или столбца из матрицы доступа D.

Мандатный механизм управления доступом позволяет корректно реализовать полномочные модели управления доступом при условии, что системой защиты реализуется требование к изоляции программных модулей (процессов) различных пользователей. То же справедливо и для дискреционного механизма, реализующего принудительное управление виртуальными каналами взаимодействия субъектов доступа.

Доказательство данного утверждения состоит в необходимости противодействовать скрытым каналам взаимодействия субъектов доступа. Если под явным каналом понимается объект, доступ к которому может быть разграничен, то под скрытым — любые иные возможности взаимодействия субъектов доступа, которые в этом случае должны исключаться, например, передача информации между субъектами доступа через буфер обмена и т.д. Очевидно, что если существует возможность передачи информации между процессами, запускаемыми с правами пользователей, которым назначены различные метки безопасности, то реализуется возможность переноса информации из объекта более высокого уровня конфиденциальности в объект более низкого уровня конфиденциальности.

Данное требование относится к процессам прикладных пользователей (которым назначаются метки безопасности). Поэтому, в первую очередь, данное требование выдвигается при реализации системы защиты для ОС семейства UNIX, где одновременно в системе могут быть запущены *процессы* различных пользователей. Для ОС семейства Windows одновременно запускаются процессы двух пользователей — текущего прикладного

пользователя и виртуального пользователя "СИСТЕМА" (системные процессы). Однако, так как системные процессы не имеют средств управления пользователем, то выполнение рассматриваемого требования для ОС семейства Windows становится неактуальным.

Отметим, что мандатный механизм управления доступом может применяться лишь для реализации канонических матриц доступа. Для реализации частных матриц доступа мандатный механизм должен функционировать в диспетчере наряду с дискреционным механизмом. Дискреционный механизм здесь служит для разграничения прав доступа пользователей, обладающих одинаковой меткой безопасности. Проиллюстрируем сказанное простым примером. Рассмотрим частную матрицу, представленную ниже.

$$D = \begin{array}{c} \\ O_1 \\ O_2 \\ \dots \\ O_{k-1} \\ O_k \end{array} \begin{array}{c} \begin{array}{cccccc} C_1 & C_2 & \dots & C_{k-1} & C_k \end{array} \\ \begin{bmatrix} Зп/Чт & Д & & Д & Д \\ Чт & Зп/Чт & & Д & Д \\ \dots & \dots & \dots & \dots & \dots \\ Чт & Чт & & Зп/Чт & Д \\ О & Чт & \dots & Чт & Зп/Чт \end{bmatrix} \end{array}$$

Чтобы реализовать данную матрицу доступа в дополнение к мандатному механизму управления доступом, реализующему каноническую полномочную модель управления доступом с комбинированным управлением виртуальными каналами взаимодействия субъектов доступа, следует запретить дискреционным механизмом управления доступом чтение субъектом С1 объекта Ok (закрыть соответствующий пассивный симплексный канал взаимодействия субъектов доступа Ck -» С1).

Таким образом, обобщая сказанное, отметим, что **мандатный механизм управления доступом можно рассматривать как альтернативный дискреционному механизму способ реализации полномочных моделей управления доступом. Более того, с точки зрения реализуемых возможностей управления доступом данные механизмы адекватны при условии реализации одной и той же матрицы доступа.**

Преимуществом мандатного механизма является интуитивная понятность, а как следствие, и простота настройки диспетчера доступа в предположении, что интуитивно понятен механизм включения шкалы полномочий и назначения меток безопасности. При этом не требуется задания в диспетчере доступа матрицы доступа как таковой. Достаточно задать правила доступа, соответствующие реализуемой полномочной модели управления доступа, и метки безопасности.

Недостатком мандатного механизма является необходимость в общем случае наряду с мандатным механизмом использовать дискреционный механизм управления доступом. То есть реализация диспетчера доступа усложняется и остается необходимость в том или ином виде задания матрицы доступа.

Выше было показано, что все функции управления доступом (все матрицы доступа и соответствующие модели) могут быть реализованы дискреционным механизмом. При этом мандатный механизм является частным случаем дискреционного и задает лишь некоторые правила. Эти правила с одной стороны упрощают администрирование диспетчера доступа (за счет включения меток безопасности), а с другой стороны ограничивают возможные ошибки в администрировании. Реализуется это за счет выполнения мандатным механизмом следующего требования: любой субъект и объект доступа, которому не присвоена метка безопасности, автоматически исключается из схемы управления доступа (какой-либо доступ непомеченного субъекта/доступ к непомеченному объекту — невозможны). При этом одно из основных требований мандатного механизма управления доступом - управление потоками может быть реализовано только в рамках канонической модели, а разграничение диспетчером доступа должно осуществляться для всех субъектов ко всем объектам доступа на защищаемом объекте.

Выводы

Рассмотренные модели и правила политики управления доступом к ресурсам локальных сетей Intranet, а также механизмы их реализации позволяют сделать следующие выводы и рекомендации.

1. В локальной сети Intranet реализуется политика защиты информации, "владельцем" которой априори не является ее пользователь, можно говорить только о защите "компьютерных данных", собственником которых пользователь не является, но может быть только их санкционированным и дисциплинированным владельцем, и только по полномочиям, предоставленным ему администратором безопасности или владельцем.

2. Наиболее широкое применение в локальных сетях Intranet получили дискреционная и мандатная модели управления доступом. Рассмотренные в статье механизмы реализации этих моделей и правила управления доступом к ресурсам сети Intranet могут быть полезны для ее пользователей, администраторов безопасности и владельцев локальных сетей Intranet.

3. Материалы стать могут использоваться для гармонизации законодательства Украины с нормами права и рекомендациями Конвенции Совета Европы о киберпреступности, например, в части международного сотрудничества в борьбе с преступлениями против конфиденциальности (несанкционированного ознакомления), целостности (несанкционированного изменения) и доступности (несанкционированного ограничения) компьютерных данных и систем.

Список литературы

1. НД ТЗІ 1.4-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.

2. НД ТЗІ 1.4-005-99. Класифікація автоматизованих систем і стандартні профілі захищеності інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.

3. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

4. НД ТЗІ 1.1-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. ДСТСЗІ СБУ, 2000.

5. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. — Москва, 1992.

6. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.

7. *Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л.* Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003. – 316 с.

8. *Шорошев В.В.* Перспективный метод защиты информационных ресурсов корпоративных сетей Интранет. Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні", НТУ України "КПІ", Міносвіти і науки України, ДСТСЗІ СБ України, випуск № 7, 2003. -С. 62-77.

9. *Шорошев В.В.* Методичні основи формування політики безпеки комп'ютерних систем. Науково-виробничий журнал Держадміністрації зв'язку та інформатизації України "Зв'язок", 2006. -№ 6. -С. 41-44.

10. *Шорошев В.В.* Основи формування політики безпеки комп'ютерних систем. Изд.."Бизнес и безопасность", 2006. -С. 141.

11. *Павличенко И.П., Щеглов А.Ю.* Новые технологии защиты вычислительных систем. Механизмы разграничения прав доступа к файловой системе и обеспечения замкнутости программной среды//Информационные технологии, 2002. — №12.

12. *Щеглов А.О.* Защита компьютерной информации от несанкционированного доступа. Изд. Наука и Техника, С.-Петербург, 2004. -С. 384.

13. *Мельников В.* Защита информации в компьютерных системах — М.: Финансы и статистика; Электроинформ, 1997.

14. *Шорошев В.В.* Перспективный метод защиты информационных ресурсов корпоративных сетей Интранет. Бизнес и безопасность, 2003. -№ 6. -С. 38-46.

Поступила 14.11.2006 г.

УДК 004.681.3 **Гайша О.О.**

РОЗРОБКА МЕТОДИКИ МОДЕЛЮВАННЯ АЛГОРИТМІВ РОБОТИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка задачі

Усі системи захисту інформації (далі по тексту – СЗІ) в основі своєї роботи мають якісь алгоритми, що виконують певні дії над зовнішніми вхідними даними та компонентами системи. Звичайно при розробці або аналізі СЗІ виникає потреба у наочному представленні послідовності дій алгоритму. Схематичне зображення надає чимало переваг порівняно з текстовим описом та математичною моделлю. Використовуючи різні рівні деталізації, можна проводити поступовий синтез/аналіз алгоритму роботи як завгодно складної системи.

Таким чином, при проектуванні СЗІ зручно використовувати графічні схеми її роботи. Однак можливі різні види і методи представлення такої інформації. Проаналізуємо наявні методики і запропонуємо авторську методику візуалізації алгоритмів СЗІ.

Аналіз посилань

Звичайним підходом для відображення будь-яких алгоритмів (в т.ч. і алгоритмів роботи СЗІ) є побудова блок-схем, згідно [1]. Рівень варіювання деталізації такого відображення не є дуже високим, і, звичайно одному графічному блокові може відповідати один чи кілька послідовних однотипних операторів програми. Таким чином, адекватне зображення більш укрупнених блоків, що реалізують певні логічні операції стає утрудненим і звичайно процес унаочнення спрощується до побудови прямокутників із вписаним текстом. Цей текст звичайно відображує назву якого-небудь процесу, що є черговою стадією послідовності дій алгоритму. Головним недоліком такого підходу є відсутність інформації про те, над чим виконується та чи інша операція, і куди передаються її результати. Таким чином, відсутня інформація про потоки даних. Можна сказати, що такий підхід добре підходить для відображення простих за змістом алгоритмів високого рівня абстракції. Для описання якихось складних (заплутаних) дій, як, наприклад, криптографічних протоколів або схем, цей метод унаочнення непридатний.

Ще одним близьким способом унаочнення є відображення схеми процесу за допомогою графу [2]. Принципово такі схеми можуть як завгодно детально відображувати логіку роботи програми (замінюючи вузли графу на більш деталізовані підграфи), але мають суттєвий недолік. У графі кожна вершина зображується у вигляді точки з порядковим номером, і для розуміння роботи програми слід весь час звертатися до таблиці відповідності вершин графа процесам або станам СЗІ. Оскільки існує можливість створення схем різного рівня деталізації, то така особливість на думку автора є значним недоліком, що перешкоджає швидкому розумінню структури графу. Крім того, кожному ребру орієнтованого графа відповідає певна операція над даними, однак не має механізму відображення, що саме це за