ФГБОУ ВПО «Воронежский государственный
технический университет»

С.С. Куликов

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Утверждено Редакционно-издательским советом
университета в качестве учебного пособия

Воронеж 2015

УДК 004.056

Куликов С. С. Модели безопасности компьютерных систем: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (2,71 Мб) / С. С. Куликов. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015. – 1 электрон. опт. диск (CDROM). – Систем. требования: ПК 500 и выше; 256 Мб ОЗУ; Windows XP; Adobe Reader; 1024x768; CD-ROM; мышь. – Загл. с экрана.

Рассмотрены сущность и понятие информации, информационной безопасности и характеристика ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегия развития информационного общества в России; международная, национальная и ведомственная нормативная правовая база в области информационной безопасности; классификация угроз и уязвимостей; стандарты в области информационной безопасности.

Издание соответствует требованиям Федерального государственного образовательного стандарта высшего профессионального образования по специальности 090301 «Компьютерная безопасность», дисциплине «Модели безопасности компьютерных систем».

Табл. 4. Ил. 32. Библиогр.: 17 назв.

Рецензенты: Концерн «Созвездие»
(канд. техн. наук, ведущий науч. сотрудник О. В. Поздышева);
д-р техн. наук, проф. А. Г. Остапенко

ВВЕДЕНИЕ

С самого начала компьютерной эры одной из основных задач для разработчиков информационных технологий стала задача обеспечения безопасности. Ни одна существующая коммерческая или государственная электронная система не может обходится без защиты собственной информации от несанкционированного доступа. Начиная с 70-х годов прошлого века в мире стали разрабатываться различные концепции и методы защиты информации, что вскоре привело к созданию единообразного подхода к этой проблеме: были разработаны первые политики безопасности.

На сегодняшний день уже положения законов и подзаконных актов в области обеспечения безопасности информационных технологий определяют ряд требований к механизмам защиты в автоматизированных системах, в том числе к механизмам логического разграничения доступа. Вместе с тем, практической реализации таких требований в современных системах препятствует то обстоятельство, что управление настройками подобных механизмов, как правило, осуществляется без должного анализа последствий. Изменения в настройки вносятся локально, модифицируются небольшие фрагменты правил логического разграничения доступа. При этом оценка влияния таких изменений на защищенность компьютерной системы в целом зачастую не производится. Данное учебное пособие содержит материал, позволяющий будущему специалисту моделировать и анализировать безопасность компьютерных систем с учетом всех требований и факторов.

1. ИСХОДНЫЕ ПОЛОЖЕНИЯ ТЕОРИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1.1. Содержания и основные понятия компьютерной безопасности

1.1.1. История развития теории и практики обеспечения компьютерной безопасности

Проблемы и задачи обеспечения безопасности информации, сохранности информационных ресурсов, охраны разного рода тайн возникли и решались задолго до компьютерной эры. Однако массовая компьютеризация всех сфер жизни, постепенный перевод основных информационных потоков в производстве и управлении в компьютерную форму и в компьютерные технологии обусловили качественные изменения той роли, которую играет безопасность и защита информации.

Современные компьютерные информационные технологии, предоставив новые, немыслимые ранее инфраструктуру и инструментарий жизнедеятельности и коммуникаций, качественно изменили и обострили проблему безопасности информации. Возможности несанкционированного доступа к информации, возможности несанкционированного получения и, как правило, без существенных организационных и материальных затрат огромных массивов данных, составляющих в ряде случаев ценнейшие корпоративные ресурсы, возможности мгновенного разрушения информационных ресурсов, хранящихся или использующихся в компьютерной форме, предопределили перевод задач обеспечения безопасности информации из разряда вспомогательных, обеспечивающих, в число основных приоритетов и условий.

В практическом плане задачи обеспечения безопасности компьютерной информации возникли в 70-х годах в связи с созданием и внедрением автоматизированных информационных систем в процессы информационного обеспечения деятельности крупных и средних предприятий и

организаций. Потребовалась теоретическая база, программно-технические решения и механизмы обеспечения безопасности при коллективной обработке общих информационных ресурсов. Именно в то время появились первые работы по политике (методологии) и моделям защиты компьютерной информации. Такие исследователи, как Л. Дж. Хоффман, Р. Хартсон, М. Харрисон, У. Руззо, Дж. Ульман, Д. Белл, Л. ЛаПадула и др., внесли значительный вклад в создание теории безопасности компьютерной информации. В этом же ряду нельзя не упомянуть отечественных исследователей того периода, в частности В. Герасимова, В. Владиславского и В. Герасименко, внесших свой вклад в исследование теоретических основ компьютерной безопасности.

Сформировались три составляющих и, соответственно, три, хотя и взаимосвязанных, но различных направления защиты компьютерной информации – обеспечение конфиденциальности информации, обеспечение целостности данных, обеспечение сохранности и работоспособности данных.

Вероятно, ввиду того, что наиболее сильные потребности в защите компьютерной информации в тот период исходили из военной сферы, основное внимание исследователей было сосредоточено на проблемах обеспечения конфиденциальности данных, основным ключом к разрешению которых были выбраны позаимствованные из "бумажной" сферы методы ограничения и разграничения доступа. В результате проблема разграничения доступа к данным с той поры и по сей день стала центральным элементом систем безопасности компьютерной информации.

К концу 70-х годов были разработаны исходные модели безопасности компьютерных систем, обеспечивающие те или иные из трех составляющих безопасности информации, и программно-технические решения построения и функционирования защищенных компьютерных систем, в частности, технологии и протоколы парольной аутентификации, криптографические методы и средства

защиты информации и т. д. Одной из наиболее известных работ, представившей обобщенный анализ теоретических и практических аспектов защиты компьютерной информации того периода стала вышедшая в 1977 году книга Л. Дж. Хоффмана «Современные методы защиты информации».

Созданные в тот период модели дискреционного и мандатного разграничения доступа послужили методологической основой для разработки первых стандартов безопасности компьютерных систем, в частности, известной «оранжевой книги», впервые опубликованной в 1983 г. Кроме того, исходные модели дискреционного разграничения доступа, в частности модель Хариссона-Руззо-Ульмана, модель мандатного (полномочного) доступа Белла-ЛаПадулы явились основой для последующих исследований, повлекших разработку новых подходов к разграничению доступа в 80-е и 90-е годы. Свой вклад в развитие моделей разграничения доступа этого периода внесли Дж. МакЛин, К. Лендвер, Дж. Гоген, Дж. Мезигер, В. Варахараджан и др.

В 90-е годы к исследованиям процессов защиты компьютерной информации более активно подключились отечественные исследователи. В этом ряду следует отметить, прежде всего, труды В. А. Герасименко, разработавшего системно-концептуальный подход к обеспечению информационной безопасности автоматизированных систем обработки данных. А. А. Грушо и Е. Е. Тимонина представили доказательный подход к проблеме гарантированности защиты информации в компьютерной системе, а также провели математический анализ ряда задач и решений в теории защиты информации применительно к различным разновидностям компьютерных систем. А. А. Грушо в сферу исследований были введены новые виды так называемых скрытых каналов утечки информации, основывающихся на использовании статистических характеристик работы компьютерной системы. В работах С. П. Расторгуева и А. Ю. Щербакова была представлена теория разрушающих программных воздействий, составившая теоретическую базу методов и механизмов

борьбы с вредоносными программными средствами. Кроме того, А. Ю. Щербаковым на основе положений исходных моделей разграничения доступа была разработана стройная субъектно-объектная модель компьютерной системы, на базе которой сформированы фундаментальные для сферы защиты информации и, в особенности, для процессов разграничения доступа понятия информационных потоков и доступов в компьютерной системе.

Заметный вклад в исследование теоретических основ компьютерной безопасности внесли представители Санкт-Петербургской научной школы во главе с П. Д. Зегждой и научной школы Института криптографии, связи и информатики (ИКСИ) Академии ФСБ России во главе с Б. А. Погореловым. В частности, под руководством П. Д. Зегжды разработана таксонометрия брешей и изъянов в системах защиты компьютерных систем. В практических разработках специалистов Санкт-Петербургской школы представлен также целый ряд интересных технических решений по созданию защищенных компьютерных систем, в частности, организационно-иерархическая система разграничения доступа.

Представителями школы ИКСИ (П. Н. Девянин, Д. И. Правиков, А. Ю. Щербаков, С. Н. Смирнов, Г. В. Фоменков и др.) помимо исследований в сфере криптографической защиты информации был проведен анализ решений и механизмов защиты информации в основных разновидностях компьютерных систем, подготовлена целая серия учебных изданий, что позволило сформировать методическую базу подготовки специалистов в сфере компьютерной безопасности.

1.1.2. Содержание и структура понятия компьютерной безопасности

Понятие компьютерной безопасности является видовым по отношению к более широкому (родовому) понятию «информационная безопасность», под которой понимается

состояние защищенности информационной сферы (предприятия, организации, общества, государства) от внутренних и внешних угроз.

Методологический анализ родового понятия «информационная безопасность» показывает, что ключевыми является следующие аспекты – информационная сфера (объект), угрозы (внутренние и внешние) и состояние защищенности (предмет объекта).

В этой логике сфера понятия «компьютерная безопасность» сужается до объекта, именуемого **«компьютерной системой»**, под которой будем понимать человеко-машинную систему, представляющую совокупность электронно-программируемых технических средств обработки, хранения и представления данных, программного обеспечения (ПО), реализующего информационные технологии осуществления каких-либо функций, и информации (данных). В развитии этой логики, под **компьютерной безопасностью** понимается состояние защищенности (безопасность) информации (данных) в компьютерных системах и безотказность (надежность) функционирования компьютерных систем. В результате составляющими компьютерной безопасности выступают безопасность информации (данных), накапливаемых, обрабатываемых в компьютерной системе, и безопасность (безотказность, надежность) функций КС.

Содержательный анализ самого понятия «информация» (сведения (сообщения, данные) независимо от формы их представления), особенностей процессов и технологий ее сбора, обработки, хранения, представления и выдачи показывает, что безотносительно к функционально-содержательной стороне работы с информацией (данными) понятие **«безопасность информации»** включает три составляющих:

- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности.

При этом под **конфиденциальностью** информации понимается специфическое свойство отдельных категорий (видов) информации, которое субъективно устанавливается ее обладателем, когда ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц, при условии того, что обладатель принимает меры по организации доступа к информации только уполномоченных лиц. Таким образом, обеспечение безопасности информации в КС означает, в первую очередь, обеспечение ее конфиденциальности (если характер информации является таковым, т.е. конфиденциальным), заключающееся в обеспечении такого порядка работы с информацией, когда она известна только определенному установленному кругу лиц (пользователей КС).

Под **целостностью** информации (данных) понимается неискаженность, достоверность, полнота, адекватность и т.д. информации, т.е. такое ее свойство, при котором содержание и структура данных определены и изменяются только уполномоченными лицами и процессами. Таким образом, обеспечение безопасности информации в КС означает в т.ч. такой порядок и технологию работы с ней, когда информация изменяется, модифицируется только уполномоченными лицами и в процессах ее передачи, хранения не возникают (устраняются) искажения, ошибки.

И, наконец, под [правомерной] **доступностью** информации (данных) понимается такое свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию обладателем или уполномоченными лицами. В результате безопасность информации в КС, в т. ч., обеспечивается ее сохранностью, способностью к восстановлению при сбоях и разрушениях, а также в отсутствии препятствий работы с ней уполномоченных лиц.

Важно подчеркнуть, что только одновременное обеспечение всех трех составляющих (конфиденциальности, целостности и доступности) дает состояние безопасности

информации. Термин «защищенность» в большинстве случаев является тождественным термину «безопасность».

Второй стороной компьютерной безопасности в рамках приведенного выше определения является безопасность (безотказность, надежность) функций компьютерных систем.

Суть и особенности такого специфического инструментария человеческой деятельности, как «компьютерные системы», в свою очередь, определяют две составляющие безопасности функций КС:

- обеспечение безотказности реализации функций;
- обеспечение аутентичности реализации функций.

Первая составляющая определяется безотказностью оборудования (технических средств обработки, хранения, передачи и представления информации) и безотказностью программного обеспечения (отсутствие сбоев в работе программного обеспечения).

Вторая составляющая (аутентичность функций) определяется целостностью ПО и целостностью программно-аппаратной конфигурации КС (параметров, настройки, состава ПО и оборудования).

При этом следует отметить, что две составляющие компьютерной безопасности являются взаимозависимыми. В частности, при нарушении безопасности информации в КС (нарушении конфиденциальности, целостности и/или доступности данных) в большинстве случаев нарушается (не обеспечивается) безопасность функций КС. Однако обратное в общем случае неверно. Иначе говоря, информация КС может находиться в безопасном состоянии с т. зр. ее конфиденциальности, целостности и сохранности, но в результате сбоев оборудования или ПО, нарушения целостности ПО или целостности программно-аппаратной конфигурации, функции КС не будут реализовываться или будут реализовывать неадекватно.

Следует также отметить, что в силу исторических особенностей развития электронно-вычислительной техники, две составляющие компьютерной безопасности

рассматривались и развивались в определенной степени независимо и параллельно, и более того, вторая составляющая (безопасность функций) рассматривалась в контексте обеспечения надежности вычислительной техники (оборудования и программного обеспечения). Исходя из этого, и в литературе, и в стандартах, в т. ч. в настоящее время под компьютерной безопасностью понимается в первую очередь (и в основном) первая ее составляющая, т.е. безопасность информации в КС.

Этого же подхода будем придерживаться и в рамках данного курса, поскольку методы и механизмы обеспечения функций КС в контексте безотказности оборудования и программного обеспечения являются предметом рассмотрения других дисциплин.

Таким образом, предметом изложения в дальнейшем будут методы, механизмы, их математическая формализация (модели), которые обеспечивают при воздействии угроз конфиденциальность, целостность и [правомерную] доступность информации в компьютерных системах.

1.1.3. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

На основе анализа теоретических и практических аспектов обеспечения компьютерной безопасности можно выделить ряд **общих принципов** создания и эксплуатации защищенных компьютерных систем (в которых обеспечивается безопасность информации).

Принцип **разумной достаточности**. Внедрение в архитектуру, в алгоритмы и технологии функционирования КС защитных механизмов, функций и процедур объективно вызывает дополнительные затраты, издержки при создании и эксплуатации, ограничивает, снижает функциональные возможности КС и параметры ее эффективности (быстродействие, задействуемые ресурсы), вызывает неудобства в работе пользователям КС, налагает на них

дополнительные нагрузки и требования — поэтому защита должна быть разумно достаточной (на минимально необходимом уровне).

Принцип **целенаправленности**. Заключается в том, что применяемые меры по устранению, нейтрализации (либо обеспечению снижения потенциального ущерба) должны быть направлены против перечня угроз (опасностей), характерных для конкретной КС в конкретных условиях ее создания и эксплуатации.

Принцип **системности**. Выбор и реализация защитных механизмов с должны производиться с учетом системной сути КС, как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое функциональных, программных, технических, организационно-технологических подсистем.

Принцип **комплексности**. При разработке системы безопасности КС необходимо использовать защитные механизмы различной и наиболее целесообразной в конкретных условиях природы – программно-алгоритмических, процедурно-технологических, нормативно-организационных, и на всех стадиях жизненного цикла – на этапах создания, эксплуатации и вывода из строя.

Принцип **непрерывности**. Защитные механизмы КС должны функционировать в любых ситуациях в т. ч. и внештатных, обеспечивая как конфиденциальность, целостность, так и сохранность (правомерную доступность).

Принцип **управляемости**. Подсистема безопасности КС должна строиться как система управления – объект управления (угрозы безопасности и процедуры функционирования КС), субъект управления (средства и механизмы защиты), среда функционирования, обратная связь в цикле управления, целевая функция управления (снижение риска от угроз безопасности до требуемого (приемлемого) уровня), контроль эффективности (результативности) функционирования.

Принцип **сочетания унификации и оригинальности**. С одной стороны, с учетом опыта создания и применения АИС,

опыта обеспечения безопасности КС должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения. С другой стороны, с учетом динамики развития ИТ, диалектики средств нападения и развития должны разрабатываться и внедряться новые оригинальные архитектурные, программно-алгоритмические, организационно- технологические решения, обеспечивающие безопасность КС в новых условиях угроз, с минимизацией затрат и издержек, повышением эффективности и параметров функционирования КС, снижением требований к пользователям.

Организационно-технологический и человеко-машинный характер природы КС определяют обширный набор методов и механизмов обеспечения информационной безопасности (рис. 1.1).

В первую очередь можно выделить ряд методов и механизмов, непосредственно обеспечивающих конфиденциальность, целостность и доступность данных, такие как разграничение доступа к данным, контроль и управление информационной структурой данных, контроль и обеспечение ограничений целостности данных, механизмы криптографического скрытия данных (шифрования), механизмы ЭЦП, обеспечивающие целостность данных в процессах их передачи и хранения, а также механизмы контроля и удаления остаточной информации на носителях данных после завершения их обработки и в освобождаемых областях оперативной памяти.

Также важнейшее значение для обеспечения компьютерной безопасности имеют методы и механизмы общесистемного характера, которые можно разделить на общеархитектурные и инфраструктурные с точки зрения программно-технической структуры современных КС.

Рис. 1.1. Систематика методов и механизмов обеспечения компьютерной безопасности

Основополагающими среди общеархитектурных являются механизмы идентификации и аутентификации, обеспечивающие исходный и обязательный рубеж безопасности в КС, методы и механизмы управления памятью, изоляции процессов и управления транзакциями в клиент-серверных системах.

Не менее важное значение имеют методы и механизмы инфраструктурного характера, в особенности для обеспечения информационной безопасности в распределенных КС – контроль и управление программно- технической конфигурацией КС, управление сеансами работы пользователей, управление доступом пользователей с рабочих станций КС, управление (контроль) сетевыми соединениями в КС, управление инфраструктурой сертификатов криптоключей,

обеспечивающих механизмы шифрования данных и электронно-цифровой подписи.

Обязательными для обеспечения информационной безопасности КС, находящими отражение в стандартах защищенности, имеют методы и механизмы обеспечивающего (профилактирующего) характера, среди которых, в первую очередь следует отметить методы протоколирования и аудита событий, методы и механизмы резервирования и архивирования, журнализации процессов изменения данных. Следует также отметить важность механизмов профилактики носителей данных их учета и контроля в организационно-технологическом контуре КС. Кроме того, человеко-машинный характер природы КС как особого инструментария деятельности предопределяет существенное значение для обеспечения информационной безопасности нормативно-организационной регламентации использования (эксплуатации) КС, процедур обучения, нормативно-административного побуждения и принуждения пользователей по вопросам обеспечения безопасности.

1.2. Угрозы безопасности в компьютерных системах

1.2.1. Понятие угроз безопасности, их классификация и идентификация

Понятие угрозы безопасности является наряду с понятием безопасности информации краеугольным камнем в сфере компьютерной безопасности, поскольку выбор защитных механизмов определяется исходя из целей устранения, нейтрализации угроз, снижения последствий (ущерба) от их возможного проявления и воздействия.

Под **угрозой безопасности** КС будем понимать совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, [правомерной] доступности информации и/или снижения надежности [безотказности и аутентичности] реализации функций КС.

Сложная и многогранная природа рассматриваемых объектов безопасности (компьютерные системы и информация в них) определяют огромное число факторов, условий, которые составляют или могут составить угрозы безопасности. Как и в других подобных случаях, когда рассматривается большое или неопределенное количество объектов, важную познавательную и прикладную роль играет **систематизация** (приведение в систему, т.е. в нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей; выстраивание в определенный порядок).

Частным случаем систематизации выступает **классификация** – последовательное деление понятий (предметов исследования), проводимое по характеристикам и параметрам, существенным с точки зрения исследовательской задачи.

На рис. 1.2 приведена классификация угроз компьютерной безопасности по различным критериям (основаниям) – по природе происхождения, по направлениям осуществления, по объекту воздействии, по способу осуществления и т.д.

Как видно из приведенной схемы, действительно угрозы компьютерной безопасности характеризуются различной природой, признаками и т.д., и поэтому классификационные схемы играют важную познавательско-исследовательскую роль.

Различают два вида классификационного (систематизированного) деления – таксономическое (родоводовое), представленное на рис. 1.2, и мереологическое (по принципу «часть-целое»).

При таксономическом делении предмет исследования (все многообразие, вся возможная совокупность элементов/экземпляров предмета исследования) разделяется на классы-таксоны, так, чтобы любой экземпляр/элемент обязательно попал какой-либо класс (т.е. для него нашелся бы класс), и так, чтобы один экземпляр/элемент попадал бы только

и только в один класс (т.е. так, чтобы одновременно не попадал в два или несколько классов).

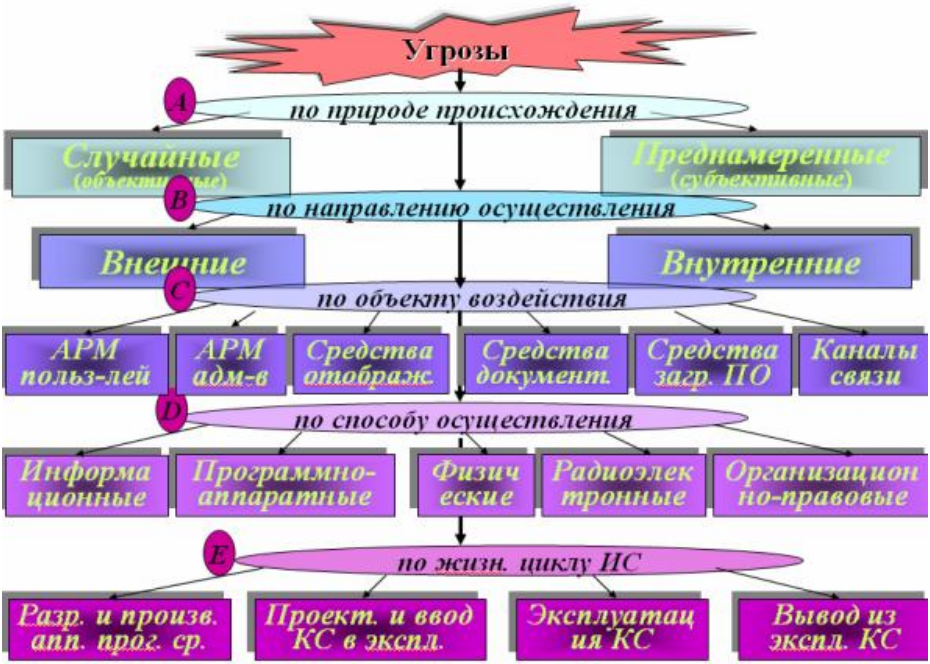

Рис. 1.2. Схема классификации угроз компьютерной безопасности по различным критериям (основаниям)

В теоретико-множественной трактовке таксономическое классификационное деление означает разбиение множества на два или более непересекающихся подмножеств, объединение которых дает полное исходное множество, а пересечение – пусто:

$$\boldsymbol{O} = \boldsymbol{O}_1 \cup \boldsymbol{O}_2 , \qquad \boldsymbol{O}_1 \cap \boldsymbol{O}_2 = \varnothing .$$

Принцип разбиения множества на классы называется критерием (основанием) **классификации**. Его выбор/обоснование определяется природой объектов исследования, а также самой исследовательской целью

(задачей), и является наиболее сложной, как правило, неформализуемой стороной построения классификационных схем. Иначе говоря, критерий (основание) классификации определяется на эвристической основе.

Во многих случаях систематизация объектов исследования по таксономически-классификационным схемам включает многоуровневое деление, когда выделенные классы, в свою очередь, разбиваются на подклассы и т.д. При этом должны обеспечиваться два правила таксономического деления – в рамках данного классы подклассы должны выделяться на основании одного и того же критерия (ошибка классификации – «сбивчивое деление», когда один подкласс выделен по одному основанию, другой подкласс этого же класса по другому основанию); и второе правило – основания для разбиения на подклассы в разных классах должны быть одноуровневого характера (ошибка классификации – «скачок в делении»).

Кроме теоретико-познавательных функций классификационные схемы (в данном случае классификационные схемы угроз) обеспечивают важные прикладные функции, а именно – полноту анализа при идентификации угроз для конкретной компьютерной системы. Поясним сказанное. Поскольку правильно построенная таксономическо-классификационная схема обладает свойством полноты, то, анализируя на ее основе наличие/отсутствие угроз соответствующих классов, подклассов и т.д., можно обеспечить полноту анализа при формировании подмножества угроз для данной КС. Кроме того, классификационные схемы помогают также систематизировать выбор защитных мер, которые могут устранять сразу целый класс (с соответствующими подклассами) угроз.

Подчеркнем еще раз, что вышесказанное справедливо при обеспечении полноты и правильности классификационных схем, что подлежит обоснованию/доказательству.

Отмеченный прикладной аспект классификации угроз обусловливает нормативно-методическое закрепление

составленных и апробированных в теоретическом и практическом отношении классификационных схем угроз в специальных стандартах. Сложившаяся терминология в этой области использует термин «каталогизация» угроз.

Таким образом, каталогизация угроз представляет собой составление и закрепление в стандартах таксономически-классификационных схем угроз, которые используются для идентификации угроз в процессах выбора защитных мер, методов и механизмов обеспечения безопасности при создании и эксплуатации защищенных компьютерных систем.

В качестве примера можно привести российский ГОСТ 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию», основанный на таксономической классификации всех возможных факторов, способных [негативно] воздействовать на информацию в компьютерных системах. По ГОСТ угрозы делятся на классы, подклассы, группы, подгруппы, виды, подвиды. На рис. 1.3. приведена схема классификации угроз/факторов до 3-го уровня деления (т.е. до групп факторов).

На основании каталогов, представляющие все поле угроз (все множество угроз) осуществляется определение тех из них, которые характерны, актуальны для конкретной компьютерной системы и конкретных условий ее функционирования. Данный процесс называется идентификацией угроз.

Идентификация угроз включает выявление угроз для конкретной компьютерной системы (из всех возможных), присвоение выявленным угрозам уникальных идентификаторов и **спецификацию** (описание) угроз.

Как правило, стандартами безопасности устанавливаются требования к спецификации выявленных угроз по определенному набору параметров, среди которых кроме идентификатора, требуется указать источник (природу происхождения) угрозы, активы (объекты КС), которые могут быть подвергнуты воздействию угрозы (на которые направлена

угроза), способы осуществления угрозы, возможные уязвимости, которые м.б. использованы для реализации угрозы.

Рис. 1.3. Схема классификации угроз по ГОСТ Р 51275-99

1.2.2. Методы оценивания угроз

Помимо идентификации и спецификации угроз важное значение для выбора и обоснования защитных мер играет оценивание угроз, под которым понимается формирование оценок идентифицированных и специфицированных угроз с точки зрения потерь, ущерба, возможных от реализации (воздействия) соответствующих угроз.

Основными факторами оценки являются возможность реализации угрозы и возможный ущерб от реализации угрозы. Общая схема оценки приведена на рис. 1.4.

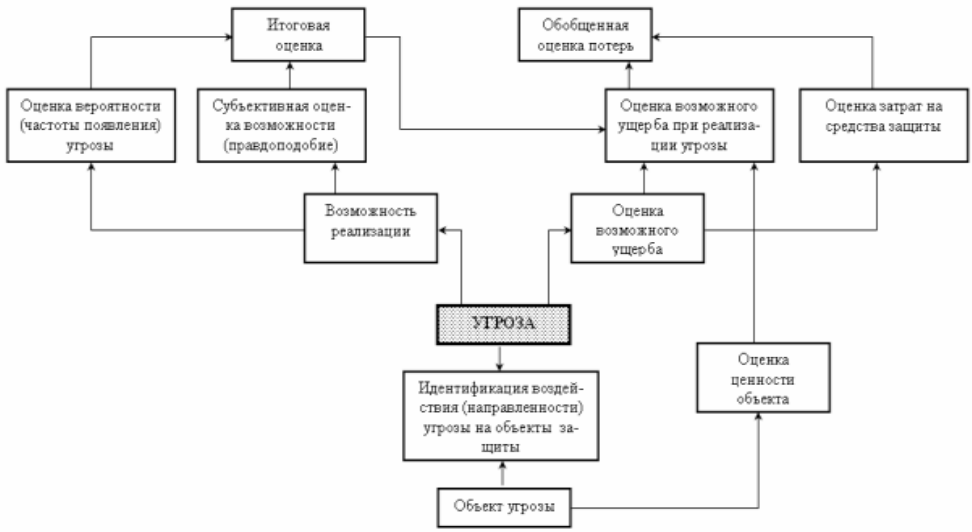

Рис. 1.4. Общая схема оценивания угроз

Основными трудностями при оценивании угроз являются проблемы выбора шкал и способов оценки по отмеченных факторам.

Естественным параметром и шкалой оценки возможности реализации угроз является оценка вероятности их реализации. Природа некоторых видов угроз позволяет вычислять эти вероятности на основе известных соответствующих физических закономерностей (априорный подход), но все же в большинстве случаев построить и обосновать аналитические соотношения для вычисления вероятностей реализации угроз не представляется возможным. К примеру, на основе Пуассоновского распределения вероятности моторных ошибок человека-оператора при вводе информации с клавиатуры вероятность угрозы, обусловленной данным фактором составляет $2 \cdot 10^{-2} \ldots 4 \cdot 10^{-3}$. Данная оценка дает

возможность определить важный параметр защитных мер, в частности, количество символов пароля и количество попыток его набора, при котором в рамках задания определенного уровня значимости ошибки 2-го рода (ошибка правильной аутентификации) легальный пользователь войдет в систему.

В некоторых случаях возможен **апостериорный** подход, основанный на накопленной статистике проявления соответствующей угрозы в данной или подобной компьютерной системе (в подобных условиях). Оценки вероятности реализации угрозы при этом вычисляются на основе методов статистических оценок.

Альтернативой аналитическому и статистическому подходу является **метод экспертных оценок**, широко используемый для оценок сложных, неформализуемых объектов.

Суть метода экспертных оценок заключается в том, что в качестве инструментария оценок (в качестве измерительного прибора) выступают специалисты-эксперты, которые на основе профессионального опыта, глубокого представления многокомпонентной природы оцениваемых объектов, дают эвристические оценки по одному или группе параметров.

В кратком изложении методика экспертных оценок включает следующие этапы.

1. Отбор экспертов (формальные и неформальные требования к специалистам-экспертам, метод «снежного кома», когда известного специалиста просят назвать других ему известных специалистов, в свою очередь, опрашивают их, и т.д. когда множество экспертов прекращает расширяться, на практике количество экспертов 10-12).

2. Выбор параметров, по которым оцениваются объекты (при этом определяются сущностные параметры оценивания, которые должны выражать природу оцениваемых объектов и быть независимыми друг от друга, определяются веса параметров).

3. Выбор шкал оценивания и методов экспертного шкалирования. Применяются порядковые, ранговые шкалы,

интервальные, абсолютные и др. шкалы. В качестве методов шкалирования выступают ранжирование объектов по предпочтительности выраженности оцениваемого параметра (порядковая шкала оценки), попарные оценки сравнительной предпочтительности во всех возможных парах оцениваемых объектов, и непосредственная оценка выраженности оцениваемого параметра (например, эксперты непосредственно дают оценку вероятности реализации угроз, в других случаях на основе специальных балльных шкал оценки).

4. Выбор и осуществление процедуры опроса экспертов (с непосредственным взаимодействием экспертов или без взаимодействия, т.н. итерационный метод опроса «Дельфи», когда эксперты непосредственно не взаимодействуют, но после каждого тура опроса им сообщают усредненные оценки прежнего тура и просят на этой основе скорректировать свои прежние оценки, исключая тем самым влияние на результаты опроса мнений конкретных «авторитетов», и т.д.).

5. Агрегирование оценок, анализ их устойчивости и согласованности, осуществляемые на основе подходов, подобных методам обработки статистических данных.

Следует отметить, что экспертные оценки, несмотря на их «субъективность» на основе хорошо подобранных экспертных комиссии, правильно установленных методов шкалирования и опроса, при соответствующей обработке дают результаты, действенность которых многократно апробированы в крупных проектах и процедурах, не допускающих другие, в особенности, аналитические и статистические подходы.

1.3. Политика и модели безопасности в компьютерных системах

1.3.1. Понятие политики и моделей безопасности информации в компьютерных системах

Фундаментальным понятием в сфере защиты информации компьютерных систем является политика безопасности. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т. д.) называют моделью безопасности.

Модели безопасности играют важную роль в процессах разработки и исследования защищенных компьютерных систем, так как обеспечивают системотехнический подход, включающий решение следующих важнейших задач:

- выбор и обоснование базовых принципов архитектуры защищенных компьютерных систем (КС), определяющих механизмы реализации средств и методов защиты информации;
- подтверждение свойств (защищенности) разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев);
- составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем.

По сути модели безопасности являются исходным связующим элементом в триаде «Заказчик (Потребитель) - Разработчик (Производитель) - Эксперт (Аудитор)». На основе моделей безопасности заказчики могут формулировать те требования к защищенным КС, которые соответствуют политике безопасности, технологическим процессам обработки информации, принятым в своих организациях и предприятиях.

Разработчики на основе моделей безопасности формируют технико-технологические требования и программно-технические решения по разрабатываемым системам. Эксперты, основываясь на моделях безопасности, строят методики и спецификации оценки защищенности конкретных систем, осуществляют сертификацию разработанных систем по требованиям защиты информации.

1.3.2. Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам

Большинство моделей разграничения доступа основывается на представлении КС как совокупности субъектов и объектов доступа.

Приведем основные положения субъектно-объектной формализации компьютерных систем в аспекте безопасности информации.

1. В КС действует дискретное время.

2. В каждый фиксированный момент времени t_k КС представляет собой конечное множество элементов, разделяемых на два подмножества:

- подмножество субъектов доступа **S**;
- подмножество объектов доступа **O**.

Определение 1.3.1. Под субъектом доступа понимается активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов.

Определение 1.3.2. Под объектом доступа понимается пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.

В модели предполагается наличие априорно безошибочного механизма различения активных и пассивных сущностей (т. е. субъектов и объектов) по свойству активности, что можно проиллюстрировать интуитивно понятными различиями между файлом с кодом программы и исполняемой (запущенной) программой, порождающей процессы над объектами системы.

Кроме того, предполагается также, что в любой момент времени t_k, в том числе и в начальный, множество субъектов доступа не пусто.

3. Пользователи КС представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.

Определение 1.3.4. Под пользователем КС понимается лицо, внешний фактор, аутентифицируемый некоторой информацией, и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет.

Таким образом, в субъектно-объектной модели понятия субъектов доступа и пользователей не тождественны. Предполагается также, что пользовательские управляющие воздействия не могут изменить свойств самих субъектов доступа, что в общем случае не соответствует реальным КС, в которых пользователи могут изменять свойства субъектов, через изменение программ (исполняемых файлов). Однако подобная идеализация позволяет построить четкую схему процессов и механизмов доступа, а угрозы безопасности, возникающие вследствие подобных реалий, рассматривать в контексте гарантий выполнения политики безопасности (политики разграничения доступа) через механизмы неизменности свойств КС (т. н. изолированная программная среда).

4. Субъекты КС могут быть порождены из объектов только активной сущностью (другим субъектом).

Определение 1.3.5. Объект o_i называется источником для субъекта s_m если существует субъект s_j, в результате воздействия которого на объект o_i возникает субъект s_m.

Соответственно, субъект s_j, называется активизирующим для субъекта s_m.

Для описания процессов порождения субъектов доступа вводится следующее обозначение:

Create (s_j, o_i)→ s_m – «из объекта o_i порожден субъект s_m при активизирующем воздействии субъекта s_j».

Create называют операцией порождения субъектов. Отметим также, что ввиду того, что в КС действует дискретное время, то под воздействием активизирующего субъекта в момент времени t_k, новый субъект порождается в момент времени t_{k+1}.

Результат операции **Create** зависит как от свойств активизирующего субъекта, так и от свойств объекта-источника. К примеру, субъект пользователя в виде работающего текстового редактора при открытии файла в формате другого текстового редактора может быть не способным активизировать находящиеся там процедуры обработки данных, а в лучшем случае быть способным только их прочитать. Другой пример – командный интерпретатор ОС по команде пользователя не может запустить на исполнение текстовый файл и создать таким образом субъект пользователя. В та- ких случаях **Create** (s_j, o_i) → ∅ .

Анализ архитектуры вычислительной системы фон Неймана, на базе которой функционируют КС, показывает, что введенное понятие субъекта доступа и процесса его порождения требует связывания субъекта с определенным объектом (объектами), отражающим состояние действующего субъекта в различные моменты времени.

Определение 1.3.6. Объект o_i в момент времени t_k ассоциирован с субъектом s_m, если состояние объекта

повлияло на состояние субъекта в следующий момент времени t_{k+1} (т. е. субъект s_m использует информацию, содержащуюся в объекте o_i).

Из определения 1.3.6 следует, что объект-источник в момент порождения субъекта является ассоциированным с ним, а в последующие моменты времени может перестать быть или остаться ассоциированным с ним. К примеру, исполняемые файлы программ являются ассоциированными с субъектом только в момент его порождения, так как в процессе инициализации (запуска) код программы из исполняемого файла копируется в специальную область памяти (сегмент кода), откуда впоследствии собственно и извлекаются команды-инструкции выполнения программы. Следовательно, файл на диске с исполняемым кодом программы после ее запуска перестает быть ассоциированным с субъектом, порожденным запуском программы. Напротив, в некоторых СУБД со встроенными системами программирования интерпретаторского типа команды-инструкции по обработке данных в каждый момент времени могут извлекаться непосредственно из файлов базы данных, располагаемых на диске. В этом случае, соответственно, файл базы данных продолжает оставаться ассоциированным с субъектом, порожденным открытием (запуском) соответствующего файла базы данных.

Активная сущность субъектов доступа заключается в их возможности осуществлять определенные действия над объектами, что объективно приводит к возникновению потоков информации. Исходя из этого, центральным положением субъектно-объектной модели является следующее.

5. Все процессы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации.

Определение 1.3.7. Потоком информации между объектом o_i и объектом o_j называется произвольная операция

над объектом o_j , реализуемая в субъекте s_m и зависящая от объекта o_i.

Для описания потоков вводят следующее обозначение:

Stream(s_m**,** o_i**)→** o_j – «поток информации от объекта o_i (o_j) к объекту o_j (o_i) в субъекте s_m (через субъект s_m)».

Поток может осуществляться в виде различных операций над объектами – чтение, изменение, удаление, создание и т. д. Объекты o_i и o_j, участвующие в потоке, могут быть как источниками, так и приемниками информации, могут быть как ассоциированными с субъектом, так и неассоциированными, а также могут быть пустыми (∅) объектами (например, при создании или удалении файлов). Следует особо подчеркнуть, что согласно определению 1.3.7 потоки информации могут быть только между объектами, а не между субъектом и объектом, в виду того, что субъект — это активная сущность, т. е. действия, процессы и т. д., а информация – пассивная сущность, которая может размещаться, извлекаться, порождаться, изменяться и т. д. только в объектах. Активная роль субъекта заключается в самой реализации потока, в его локализации в субъекте (через субъект), в том числе, через задействование в потоке ассоциированных с субъектом объектов (например, буферов оперативной памяти). В этом отношении более детальный анализ понятия субъектов доступа, определений 1.3.5 и 1.3.6 показывает, что ассоциированные объекты могут быть разделены на два вида:

• функционально-ассоциированные объекты;

• ассоциированные объекты-данные.

Функционально-ассоциированные объекты влияют (определяют) на сами процессы субъекта (например, состояние сегмента кода определяет свойства субъекта в следующий момент времени). Ассоциированные объекты-данные выступают в роли аргументов в операциях, порождающих потоки информации (например, буферы оперативной памяти, в которых помещается для отображения на экране информация

при чтении файла). Таким образом, если на первый взгляд в потоке участвует только один (одни) субъект(ы), то, как правило, при более пристальном взгляде можно увидеть, что в данной операции участвуют еще и ассоциированные с субъектом доступа объекты.

Заметим также в развитие положения 5, что, исходя из определения 1.3.7, поток всегда инициируется (порождается) субъектом доступа. На этом основании вводится следующее центральное в политике и моделях разграничения доступа понятие.

Определение 1.3.8. Доступом субъекта s_m к объекту o_j называется по- рождение субъектом s_m потока информации между объектом o_j и некоторым(и) объектом o_i (в т. ч., но не обязательно, объект o_i ассоциирован с субъектом s_m).

Формальное определение 1.3.8 понятия доступа дает возможность средствами субъектно-объектной модели перейти непосредственно к описанию процессов безопасности информации в защищенных КС. С этой целью вводится множество потоков **P** для всей совокупности фиксированных декомпозиций КС на субъекты и объекты во все моменты времени (множество **P** является объединением потоков по всем моментам времени функционирования КС).

С точки зрения процессов безопасности, трактуемой как состояние защищенности информации в КС, множество потоков P разбивается на два непересекающихся подмножества P_N и P_L:

$$\mathbf{P} = P_L \cup P_N,$$
$$P_L \cap P_N = \emptyset,$$

где P_L – множество потоков, вызываемых легальными (безопасными) доступами;

P_N – множество опасных, нарушающих состояние защищенности информации (конфиденциальность, целостность и доступность информации) потоков в КС.

На основе множества потоков дается следующее понятие, составляющее основу формализации политики разграничения доступа в моделях безопасности.

Определение 1.3.9. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие множеству P_L.

Определение 1.3.9 завершает основные положения субъектно- объектной модели КС, на методологическом фундаменте которой строится большинство моделей разграничения доступа, выражающих, собственно, подходы, принципы и механизмы правил разграничения доступа (политику разграничения доступа), а также формальные их спецификации (сами модели разграничения доступа). Ввиду того, что определение 1.3.9 не конкретизирует и не детализирует конкретных механизмов фильтрации потоков на опасные и безопасные, то можно говорить, что субъектно-объектная модель КС инвариантна относительно любой принимаемой в КС политики безопасности.

Добавим, кроме того, что во многих источниках и, в особенности, в нормативных документах по защите информации в КС, основываясь на понятии правил разграничения доступа, вводят производные термины в виде санкционированных и несанкционированных доступов.

1.3.3. Монитор безопасности и основные типы политик безопасности

Анализ практического опыта по защите компьютерной информации, а также основных положений субъектно-объектной модели КС позволяет сформулировать несколько аксиоматических условий, касающихся структуры и функционирования защищенных КС.

Аксиома 1.3.1. В защищенной КС в любой момент времени любой субъект и объект должны быть

персонифицированы (идентифицированы) и аутентифицированы.

Данная аксиома определяется самой природой и содержанием процессов коллективного доступа пользователей к ресурсам КС. Если какие- либо субъекты (пользователи) имеют возможность выдать себя в КС за других субъектов (пользователей) или если имеют возможность подменять (выдавать) одни объекты доступа за другие, то ни о какой безопасности, защищенности речи быть не может. Таким образом, аксиома 1.3.1 выражает необходимое условие безопасности (защищенности) информации в КС, а процедуры, механизмы и системы, осуществляющие идентификацию и аутентификацию пользователей, их субъектов и объектов доступа, являются исходным и важнейшим программно-техническим рубежом защиты информации в КС.

Аксиома 1.3.2. В защищенной КС должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом(ами)-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам.

В литературе для данной активной компоненты утвердился термин «монитор безопасности». Понятие монитора безопасности позволяет выразить схемотехнический аспект защиты информации в КС в виде схемы, представленной на рис. 1.5. В структуре большинства типов программных средств, на основе которых строятся информационные системы (ОС, СУБД), можно выделить ядро (ядро ОС, машина данных СУБД), в свою очередь, разделяемое на компоненту представления информации (файловая система ОС, модель данных СУБД) и на компоненту доступа к данным (система ввода-вывода ОС, процессор запросов СУБД), а также надстройку (утилиты, сервис, интерфейсные компоненты). Инициализированные субъекты при осуществлении процессов доступа обращаются за сервисом, функциями к ядру системы – см. рис. 1.5.а.

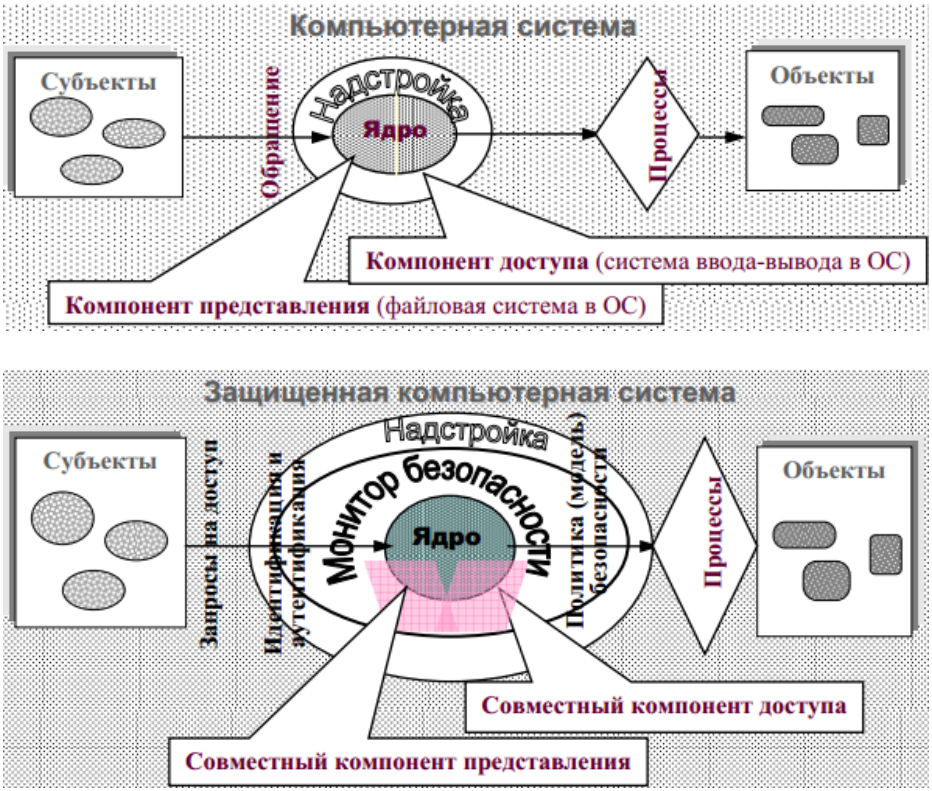

Рис. 1.5. Системотехнический аспект а) незащищенной КС, б) защищенной КС

В защищенной системе появляется дополнительная компонента, обеспечивающая процессы защиты информации, прежде всего, процедуры идентификации/аутентификации, а также управление доступом на основе той или иной политики безопасности (разграничения доступа) – см. рис. 1.5.б. Ввиду того, что как само ядро КС (компонент представления и компонент доступа), так и процессы разграничения доступа неразрывно связаны с представлением информации и манипулированием с ней, то монитор безопасности должен быть интегрирован непосредственно в ядро системы. Иногда говорят, что монитор безопасности должен быть реализован на

нулевом уровне (на уровне ядра) системы. В этом отношении заметим, что более правильный подход заключается в такой разработке компонентов ядра КС, которые бы изначально строились на основе определенной модели безопасности (модели разграничения) доступа.

В практическом плане, в том числе и с учетом отечественных и международных нормативных требований по сертификации защищенных систем, к реализации монитора безопасности предъявляются следующие обязательные требования:

1. **Полнота.** Монитор безопасности должен вызываться (активизироваться) при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.

2. **Изолированность.** Монитор безопасности должен быть защищен от отслеживания и перехвата своей работы.

3. **Верифицируемость.** Монитор безопасности должен быть проверяемым (само- или внешне тестируемым) на предмет выполнения своих функций.

4. **Непрерывность.** Монитор безопасности должен функционировать при любых штатных и нештатных, в том числе и аварийных ситуациях.

Таким образом, именно монитор безопасности в защищенной системе является субъектом осуществления принятой политики безопасности, реализуя через алгоритмы своей работы соответствующие модели безопасности. В этом отношении большое значение имеет следующее аксиоматическое положение.

Аксиома 1.3.3. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима (должна существовать) информация и объект(ы), ее содержащий(ие) (помимо информации для идентификации и аутентификации пользователей).

Из аксиомы 1.3.3 следует, что монитор безопасности, в свою очередь, как и любая активная сущность в КС, является

субъектом с соответствующим объектом-источником и ассоциированными объектами. Отсюда вытекают следующие важные следствия.

Следствие 1.3.1 (из аксиомы 1.3.3). В защищенной КС существуют особая категория субъектов (активных сущностей), которые не инициализируют и которыми не управляют пользователи системы т. н. системные процессы (субъекты), присутствующие (функционирующие) в системе изначально.

К числу подобных системных субъектов относится исходный системный процесс, который инициализирует первичные субъекты пользователей, а также монитор безопасности, который управляет доступами субъектов пользователей к объектам системы. Соответственно, для обеспечения защищенности в КС свойства системных субъектов должны быть неизменными, от чего напрямую зависят гарантии безопасности.

Следствие 1.3.2 (из аксиомы 1.3.3). Ассоциированный с монитором безопасности объект, содержащий информацию по системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной КС.

Действительно, возможность несанкционированно изменять, удалять данный объект может полностью разрушить или дискредитировать всю систему безопасности КС. Поэтому способы и особенности реализации данного объекта имеют определяющее значение для защищенности информации в КС.

Информация в ассоциированном с монитором безопасности объекте должна касаться конкретных зарегистрированных в системе пользователей и конкретных объектов системы. Следовательно, для планирования и управления системой разграничения доступа конкретного коллектива пользователей КС должна быть предусмотрена процедура доступа к данному объекту со стороны внешнего

фактора, т. е. через субъект(ы) пользователя. Отсюда вытекает еще одно следствие.

Следствие 1.3.3 (из аксиомы 1.3.3). В защищенной системе может существовать доверенный пользователь (администратор системы), субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту-данным для управления политикой разграничения доступа.

Заметим также, что субъекты, инициируемые администратором системы, не являются элементами или процессами монитора безопасности, а лишь обеспечивают монитор безопасности конкретной информацией для управления и контроля доступом субъектов к объектам системы.

Принципы, способы представления и реализация ассоциированных с монитором безопасности объектов определяются типом политики безопасности и особенностями конкретной КС.

Несмотря на то, что к настоящему времени разработано и апробировано в практической реализации большое количество различных моделей безопасности КС, все они выражают несколько исходных политик безопасности. В упрощенной трактовке политику безопасности понимают, как общий принцип (методологию, правило, схему) безопасной работы (доступа) коллектива пользователей с общими информационными ресурсами. При этом согласно определению 1.3.9 важнейшее значение имеет критерий безопасности доступов субъектов к объектам, т. е. правило разделения информационных потоков, порождаемых доступами субъектов к объектам, на опасные и неопасные.

Методологической основой для формирования политик безопасности в защищенных КС послужили реальные организационно-технологические схемы обеспечения безопасности информации во вне (до) компьютерных сферах. Многие подходы к защите компьютерной информации были «подсмотрены», в частности, в сфере работы с «бумажными»

конфиденциальными документами, проще говоря, в сфере делопроизводства.

Выделяется две основных (базовых) политики безопасности - дискреционная и мандатная. В еще не до конца устоявшейся терминологии сферы защиты компьютерной информации, первую называют политикой избирательного доступа, а вторую – политикой полномочного доступа. Следует отметить, что известные модели ролевого доступа выделяют в группу особой «ролевой политики безопасности». Кроме того, в документальных информационно-поисковых системах применяется политика тематического разграничения доступа, также как и другие политики «подсмотренная» во внекомпьютерной (библиотечно-архивной) сфере.

Модели, выражающие ту или иную политику безопасности, подробно рассматриваются в соответствующих главах. Здесь же мы ограничимся общей их характеристикой, отталкиваясь от основных понятий и, в частности, определений 1.3.8, 1.3.9 субъектно-объектной модели КС.

Политика дискреционного (избирательного) доступа. Множество безопасных (разрешенных) доступов PL задается для именованных пользователей (субъектов) и объектов явным образом в виде дискретного набора троек «Пользователь(субъект)-поток(операция)-объект».

Принцип дискреционной политики разграничения доступа можно охарактеризовать схемой «каждый-с каждым», т. е. иными словами для любой из всевозможных комбинаций «пользователь (субъект)- ресурс (объект)» должно быть явно задано («прописано») разрешение/запрещение доступа и вид соответствующей разрешенной/запрещенной операции (**Read, Write** и т. д.). Таким образом, при дискреционной политике разграничение доступа осуществляется самым детальным образом – до уровня отдельно взятого субъекта, отдельно взятого объекта доступа и отдельно взятой операции.

Политика мандатного (полномочного) доступа. Множество безопасных (разрешенных) доступов PL задается неявным образом через введение для пользователей-субъектов некоторой дискретной характеристики доверия (уровня допуска), а для объектов некоторой дискретной характеристики конфиденциальности (грифа секретности), и наделение на этой основе пользователей-субъектов некими полномочиями порождать определенные потоки в зависимости от соотношения «уровень допуска-поток(операция)-уровень конфиденциальности».

Таким образом, в отличие от дискреционной политики, при мандатной политике разграничение доступа производится менее детально – до уровня группы пользователей с определенным уровнем допуска и группы объектов с определенным уровнем конфиденциальности. Заметим также, что уменьшение гранулированности доступа создает условия для упрощения и улучшения управления доступом ввиду существенного уменьшения количества субъектов управления и контроля.

Политика тематического доступа. Множество безопасных (раз- решенных) доступов P_L задается неявным образом через введение для пользователей-субъектов некоторой тематической характеристики – разрешенных тематических информационных рубрик, а для объектов аналогичной характеристики в виде набора тематических рубрик, ин- формация по которым содержится в объекте, и наделение на этой основе субъектов-пользователей полномочиями порождать определенные потоки в зависимости от соотношения «набор тематических рубрик субъекта–набор тематических рубрик объекта».

Как и при мандатном доступе, тематический принцип определяет доступ субъекта к объекту неявно, через соотношение предъявляемых специальных характеристик субъекта и объекта и, соответственно, по сравнению с

дискреционным принципом существенно упрощает управление доступом.

Политика ролевого доступа. Множество безопасных (разрешенных) доступов P_L задается через введение в системе 1 дополнительных абстрактных сущностей – ролей, выступающих некими «типовыми» (ролевыми) субъектами доступа, с которыми ассоциируются конкретные пользователи (в роли которых осуществляют доступ), и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы.

Ролевая политика разграничивает доступ не на уровне пользователей-субъектов, а на уровне ролей, являющихся группами однотипного доступа к объектам системы, и на этой основе развивает ту или иную базовую политику безопасности (дискреционную или мандатную). Поэтому в большинстве источников ролевой принцип разграничения доступом не выделяется в отдельную политику, а рассматривается в качестве неких дополнений к моделям дискреционного или мандатного доступа.

Следует также отметить, что в практике функционирования защищенных компьютерных систем широко используется временные и маршрутные (в распределенных КС) ограничения доступа, что позволяет, в принципе, говорить о временно́й и маршрутной политике безопасности, которые, дополняют отмеченные базовые политики безопасности.

Каждая политика безопасности требует определенной информации для разграничения доступа в конкретной системе, локализуемой в объекте, ассоциированном с монитором безопасности. Для моделей дискреционного доступа эта информация представляет список разрешенных троек «субъект(пользователь)-операция-объект». Для управления доступом в системах с мандатным доступом необходима информация по уровням допуска субъектов и грифам конфиденциальности объектов. В системах ролевого доступа

помимо информации, регламентирующей доступ ролей к объектам (на основе дискреционного или мандатного принципа), необходима информация по ассоциации пользователей-субъектов с ролями. При тематическом доступе необходима информация по тематическим рубрикам пользователей-субъектов и объектов.

Конкретная модель безопасности детализирует и формализует (в виде аналитических соотношений, алгоритмов, и т. д.) общий принцип разграничения доступа на основе одной из рассмотренных политик, а иногда некоторой их совокупности. В конкретной КС разработчики строят и реализуют оригинальные программно-технические решения, воплощающие модели безопасности, в том числе структуру, функции, программно- техническое воплощение монитора безопасности.

1.3.4. Гарантирование выполнения политики безопасности

Положения субъектно-объектной модели КС, в частности, понятия доступа субъектов к объектам и политики безопасности позволяют сформулировать следующий общий критерий безопасности КС.

Определение 1.3.10. Компьютерная система безопасна тогда и только тогда, когда субъекты не имеют никаких возможностей нарушать (обходить) установленную в системе политику безопасности.

Субъектом обеспечения политики безопасности выступает монитор безопасности. Его наличие в структуре КС, соответственно, является необходимым условием безопасности. Что касается условий достаточности, то, очевидно, они заключены, несмотря на тавтологичность выражения, прежде всего, в безопасности самого монитора безопасности.

Подтверждением данного тезиса является обязательное включение в состав спецификаций по созданию (разработке) и

оценке (сертификации) защищенных КС требований корректности, верификации, адекватности и т. д. средств защиты информации (т. е. монитора безопасности) во всех, в том числе, и отечественных стандартах и руководящих документах по компьютерной безопасности.

Необходимость доказательного подхода к гарантиям обеспечения защищенности информации в КС в отечественной литературе была впервые поставлена в работах А. А. Грушо. В этих работах приведен пример гарантированно (т. е. математически доказанной) защищенной системы обработки информации на основе определенных предположений и условий.

В развитие методологии данного подхода А. Ю. Щербаковым предложена модель гарантированности выполнения политики безопасности в более широких рамках и условиях субъектно-объектной модели КС.

Приведем основные положения данной модели.

Автором модели, прежде всего, было отмечено влияние на безопасность системы не только доступов (потоков) к объектам, осуществляемых субъектами пользователей, но и того, какого типа субъектами пользователи осуществляют доступ к объектам. К примеру, доступ пользователя к файлу базы данных через СУБД порождает информационный поток одного типа с определенными регламентациями-ограничениями, а доступ к тому же файлу базы данных с помощью дискового редактора – информационный поток другого типа, через который пользователь может получить не предназначенную, вообще говоря, ему информацию. При этом с формальной точки зрения политика безопасности, определяющая правомерность самого факта доступа данного пользователя к файлу базы данных соблюдается и в том и другом случае.

Отсюда следует, что правила разграничения доступа, составляющие основу политики безопасности, должны включать и правила порождения (инициализации) пользователями субъектов доступа.

В технологическом плане выполнение данного требования приводит к необходимости расщепления монитора безопасности на два отдельных субъекта:

• монитор безопасности объектов;

• монитор безопасности субъектов.

Вводятся соответствующие определения.

Определение 1.3.11. Монитором безопасности объектов **(МБО)** называется субъект, активизирующийся при возникновении потока между любыми объектами, порождаемого любым субъектом, и разрешающий только те потоки, которые принадлежат множеству P_L .

Определение 1.3.12. Монитором безопасности субъектов **(МБС)** называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов из фиксированного подмножества пар активизирующих субъектов и объектов-источников.

Определение 1.3.12, по сути, вводит в состав политики безопасности КС в качестве дополнительной составной части специальную политику порождения пользователями субъектов доступа. Соответственно, как и у любого субъекта, у МБС должен быть объект-источник, функционально-ассоциированный объект (исполняемый код в оперативной памяти) и ассоциированный объект-данные, содержащий необходимую информацию по политике порождения пользователями субъектов доступа в системе – см. рис. 1.6.

Вторым аспектом, подмеченным в плане гарантий выполнения политики безопасности, является неизменность свойств субъектов доступа в процессе функционирования КС. Многие известные атаки на защищенные КС как раз и осуществляются по сценарию подмены кода программ, запускаемых на выполнение регламентированных функций (т. е. фактически подмены свойств субъектов). Данное требование имеет отношение к любым субъектам доступа

любых пользователей, но особо для системных субъектов, и, в частности, для монитора безопасности.

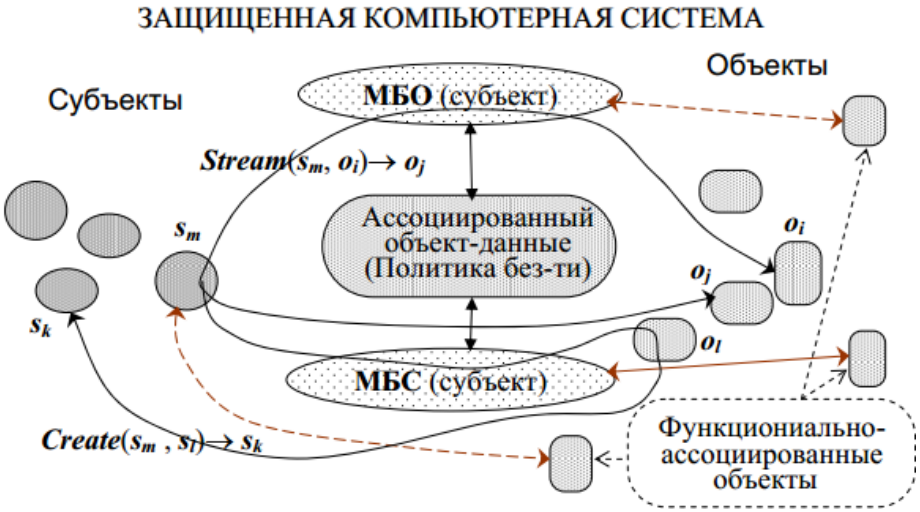

Рис. 1.6. Порождение потоков **(Stream)** и субъектов **(Create)** с учетом **МБО** и **МБС**

Для рассмотрения условий неизменности субъектов, вводятся следующие определения.

Определение 1.3.13. Объекты o_i и o_j тождественны в момент времени t ($o_i[t] \equiv o_j[t]$), если они совпадают как слова, записанные в одном языке.

Тождественность объектов по определению 1.3.13 основывается не на физической тождественности, а на тождественности до уровня последовательности символов из алфавита языка представления. Для иллюстрации понятия тождественности приведем пример эквивалентности (тождественности) двух файлов на основе побайтного сравнения, один из которых размещен на диске, другой в

оперативной памяти, и находящихся, соответственно, в разной реализации по физическим процессам функционирования носителей (т. е. являющихся физически не тождественными).

Введенное понятие тождественности объектов позволяет перейти к рассмотрению понятия тождественности и неизменности субъектов доступа.

Определение 1.3.14. Субъекты s_i и s_j тождественны в момент времени t, если попарно тождественны все ассоциированные с ними объекты.

Определения 1.3.13 и 1.3.14 неявно требуют наличия в КС специального механизма сортировки однотипных объектов и их попарного сравнения, и, кроме того, обусловливают следующее важное следствие.

Следствие 1.3.4 (из определений 1.3.13 и 1.3.14). Порожденные субъекты тождественны, если тождественны все порождающие субъекты и объекты-источники.

Обоснованность данного следствия вытекает из тождества функционально-ассоциированных объектов в порождающих субъектах, которые отвечают за порождение нового субъекта, а также из тождественности аргументов операции порождения, т. е. ассоциированных объектов-данных и объектов-источников, которые определяют свойства порождаемых субъектов.

Очевидно, что субъекты, осуществляющие доступ к объектам системы, в том числе и к объектам, ассоциированным с другими субъектами, могут тем самым влиять на них и изменять их свойства. Поэтому вводится следующее определение.

Определение 1.3.15. Субъекты s_i и s_j называются невлияющими друг на друга (или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами

o_{ik} и o_{jl}, ассоциированными, соответственно с субъектами s_i и s_j. Причем объекты o_{ik} не ассоциированы с субъектом s_j, а объекты o_{jl} не ассоциированы с субъектом s_i.

Отметим, что термин «изменение состояния объекта» в определении 1.3.15 трактуется как нетождественность (в смысле определения 1.3.13) объекта с самим собой в различные моменты времени.

Анализ понятия ассоциированных с субъектом объектов позволяет ввести еще более жесткое определение по влиянию одних субъектов на других.

Определение 1.3.16. Субъекты s_i и s_j называются абсолютно не-влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях определения 1.3.15 множества ассоциированных объектов указанных субъектов не имеют пересечения.

На основании данного определения можно сформулировать достаточное условие гарантированного выполнения политики безопасности.

Утверждение 1.3.1 (достаточное условие гарантий безопасности 1). Монитор безопасности объектов разрешает порождение потоков только из множества P_L, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Утверждение 1.3.1 для обеспечения гарантий безопасности накладывает чрезвычайно жесткие условия, практически не выполнимые на практике, или существенно снижающие функциональные возможности КС (отсутствие общих объектов-источников для запуска программ разными пользователями, отсутствие общих участков памяти, буферов для обмена данными и т. п.).

Для исследования подходов, в большей степени возможных при практической реализации, вводятся понятия

замкнутости и изолированности подмножества субъектов системы.

Определение 1.3.17. КС называется замкнутой по порождению субъектов, если в ней действует **МБС**, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников, рассматриваемых для фиксированной декомпозиции КС на субъекты и объекты.

Эквивалентным понятием для замкнутой по порождению субъектов системы является понятие «изолированной программной среды» (ИПС). Механизм замкнутой программной среды сокращает множество возможных субъектов до некоторого множества фиксированной мощности, но при этом не гарантирует отсутствие некорректных субъектов внутри замкнутой среды.

Определение 1.3.18. Множество субъектов КС называется изолированным (абсолютно изолированным), если в ней действует **МБС** и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и **МБС.**

Из данного определения вытекают следующие следствия.

Следствие 1.3.5. (из определения 1.3.18). Любое подмножество субъектов изолированной (абсолютно изолированной) КС, включающее МБС, также составляет изолированную (абсолютно изолированную) среду.

Следствие 1.3.6. (из определения 1.3.18). Дополнение изолированной (абсолютно изолированной) среды субъектом, корректным (абсолютно корректным) относительно любого из числа входящих в изолированную (абсолютно изолированную) среду, оставляет ее изолированной (абсолютно изолированной).

На этой основе можно сформулировать другое условие достаточности гарантий выполнения политики безопасности.

Утверждение 1.3.2. (достаточное условие гарантий безопасности 2). Если в абсолютно изолированной КС существует **МБО** и порождаемые субъекты абсолютно корректны относительно **МБО**, а также существует **МБС,** который абсолютно корректен относительно **МБО**, то в КС реализуется только доступ, описанный политикой разграничения доступа.

В отличие от первого условия достаточности гарантий выполнения политики безопасности, второе условие менее жестко, так как накладывает условия абсолютной корректности не на все множество возможных субъектов, а лишь на фиксированное их подмножество, образующее замкнутую (изолированную) программную среду (ИПС).

И все же, требование абсолютной корректности, хотя и для фиксированного подмножества субъектов, является также чрезвычайно жестким и трудно выполнимым на практике без существенного снижения функциональных возможностей КС.

Дальнейший анализ подходов к гарантиям безопасности, точнее, к возможностям реализации ИПС, показал необходимость включения требований по неизменности свойств субъектов, основанных на неких дополнительных процедурах, связанных с порождением субъектов.

Определение 1.3.19. Операция порождения субъектов **Create** (s_k, o_m) → s_l называется порождением с контролем неизменности объекта, если для любого момента времени t > t_0 , в который активизирована операция порождения объекта **Create**, порождение объекта s_l возможно толь- ко при тождественности объекта-источника относительно момента t_0 , т. е. при o_m[t] ≡ o_m[t_0].

Из определения 1.3.19 вытекает следующее важное следствие, имеющее непосредственное отношению к

неизменности свойств субъектов доступа, как важнейшего условия обеспечения политики безопасности в системе.

Следствие 1.3.7. (из определения 1.3.19). В условиях определения 1.3.19 порожденные субъекты $s_i[t_1]$ и $s_i[t_2]$ тождественны, если $t_1 > t_0$ *и* $t_2 > t_0$. При $t_1 = t_2$ порождается один и тот же объект.

Введение понятия порождения субъектов с контролем неизменности объектов позволяет сформулировать и доказать такое достаточное условие для обеспечения ИПС, которое может быть практически реализовано в реальных КС.

Утверждение 1.3.3. (базовая теорема ИПС). Если в изолированной КС, в которой действует порождение субъектов с контролем неизменности объекта, в момент времени t_0 через любой субъект к любому объекту существуют только потоки, не противоречащие условию корректности (абсолютной корректности), то в любой момент времени $t_k > t_0$ КС также остается изолированной (абсолютно изолированной).

Утверждение 1.3.3 имеет важнейшее значение с точки зрения достаточных условий для обеспечения гарантий выполнения политики безопасности в защищенных КС. Вместе с тем, при практической реализации условий утверждения 1.3.3 также возникает несколько серьезных проблем. Одна из них, если так можно выразиться, созвучна с известной проблемой «ахиллесовой пяты». А именно, с исходным состоянием КС, в котором должны быть только потоки, гарантирующие корректность исходных субъектов.

Проблемы и пути обеспечения исходной корректности (изолированности) КС основываются на определенных принципах и процедурах загрузки (ступенчатой инициализации) КС в начальный момент времени.

Вторая проблема связана с понижением производительности (быстродействия) КС в связи с

осуществлением процедур контроля неизменности объектов-источников при порождении субъектов.

От себя также заметим, не умаляя достоинств и теоретического значения рассмотренной модели гарантий выполнения политики безопасности, что ее авторами упущен еще один важный в практическом плане аспект. В частности, как уже отмечалось в следствии 1.3.1 из аксиомы 1.3.3, для управления конкретными параметрами системы разграничения доступа могут (должны) существовать субъекты доверенных пользователей (администраторов), имеющих доступ к ассоциированному с **МБО** объекту - данным. Однако рассмотренные выше условия гарантий безопасности основываются на понятии корректности (невлияния) относительно **МБО** и **МБС** всех субъектов доступа. Согласно определению 1.3.15 корректность субъектов обеспечивается их невозможностью изменять состояние всех ассоциированных с другими субъектами объектов, в том числе и объектов- данных, ассоциированных с **МБО**, содержащих конкретную информацию по политике разграничения доступа. Следовательно, полная и строгая реализация условий ИПС из-за невозможности впоследствии изменять ассоциированные с **МБО** объекты потребует изначального встраивания в систему конкретных параметров разграничения доступа (по конкретным и, соответственно, изначально зарегистрированным в системе пользователям, и конкретным, изначально созданным в системе объектам доступа), что лишает такую систему какой-либо универсальности и гибкости.

Тем не менее, теоретическая значимость рассмотренной модели несомненна, так как создает инвариантную основу по отношению к любым политикам и моделям разграничения доступа для гарантий выполнения политики безопасности в защищенных КС.

2. МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

2.1. Модели безопасности на основе дискретной политики

Модели безопасности, строящиеся на субъектно-объектной модели КС, еще называют моделями конечных состояний. В данных моделях инициализация информационных потоков трактуется как запросы субъектов на доступ к объектам, которые в зависимости от политики безопасности разрешаются или запрещаются. Осуществление субъектом разрешенного доступа к объекту переводит систему в следующий момент времени в другое состояние, рассматриваемое как совокупность состояний субъектов и объектов системы. Проблема безопасности в КС рассматривается с точки зрения анализа и исследования условий, правил, порядка и т. п. разрешений запросов на доступ, при которых система, изначально находясь в безопасном состоянии, за конечное число переходов перейдет также в безопасное состояние.

2.1.1. Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона

Политика дискреционного доступа охватывает самую многочисленную совокупность моделей разграничения доступа, реализованных в большинстве защищенных КС, и исторически является первой, проработанной в теоретическом и практическом плане.

Первые работы по моделям дискреционного доступа к информации в КС появились еще в 60-х годах и подробно представлены в литературе. Наиболее известные из них – модель АДЕПТ-50 (конец 60-х годов), пятимерное пространство Хартсона (начало 70-х годов), модель Хариссона-Руззо-Ульмана (середина 70-х годов), модель Take-Grant (1976 г.). Авторами и исследователями этих моделей был внесен значительный вклад в теорию безопасности

компьютерных систем, а их работы заложили основу для последующего создания и развития защищенных КС.

Модели дискреционного доступа непосредственно основываются и развивают субъектно-объектную модель КС как совокупность некоторых множеств взаимодействующих элементов (субъектов, объектов и т. д.). Множество (область) безопасных доступов в моделях дискреционного доступа определяется дискретным набором троек «Пользователь (субъект)-поток (операция)-объект».

Конкретные модели специфицируют способ представления области безопасного доступа и механизм проверки соответствия запроса субъекта на доступ области безопасного доступа. Если запрос не выходит за пределы данной области, то он разрешается и выполняется. При этом постулируется, что осуществление такого доступа переводит систему в безопасное состояние.

Специфика и значение моделей заключается в том, что исходя из способа представления (описания) области безопасного доступа и механизма разрешений на доступ анализируется и доказывается, что за конечное число переходов система останется в безопасном состоянии.

Модель дискреционного доступа, предложенная Хартсоном, вероятно наиболее наглядно в формальном плане иллюстрирует дискреционный принцип разграничения доступа, выраженный языком реляционной алгебры. Приведем ее основные положения в кратком изложении.

1. Система представляется совокупностью пяти наборов (множеств):

- множества пользователей **U**;
- множества ресурсов **R**;
- множества состояний **S**;
- множества установленных полномочий **A**;
- множества операций **E.**

2. Область безопасности представляется декартовым произведением:

$$\mathbf{A \times U \times E \times R \times S.}$$

3. Пользователи подают запросы на доступ к ресурсам, осуществление которых переводит систему в новое состояние. Запросы на доступ представляются четырехмерными кортежами

$$\mathbf{q = (u, e, R', s),}$$

где $\mathbf{u \in U, e \in E, s \in S, R' \subseteq R}$ (**R'**- требуемый набор ресурсов).

Таким образом, запрос на доступ представляет собой подпространство четырехмерной проекции пространства безопасности. Запрос удовлетворяется, если он полностью заключен в области безопасности.

4. Процесс организации доступа алгоритмически описывается следующим образом.

4.1. Определить из **U** те группы пользователей, к которым принадлежит **u**. Затем выбрать из **A** те спецификации, которым соответствуют выделенные группы пользователей. Этот набор полномочий F(**u**) определяет привилегию пользователя **u.**

4.2. Определить из множества **A** набор полномочий **P** =F(**e**), которые устанавливают e как основную операцию. Набор полномочий **P** =F(**e**) определяет привилегию операции **e.**

4.3. Определить из множества **A** набор полномочий **P** =F(**R'**), разрешающих доступ к набору ресурсов **R'.** Набор полномочий **P** =F(**R'**) определяет привилегию ресурсов **R'.**

Полномочия, которые являются общими для всех трех привилегий, образуют так называемый домен полномочий запроса **D(q)**

$$\mathbf{D(q) = F(u) \cap F(e) \cap F(R').}$$

4.4. Убедиться, что запрашиваемый набор ресурсов **R'** полностью содержится в домене запроса **D(q)**, т. е. любой **r** из набора **R'** хотя бы один раз присутствует среди элементов **D(q)**.

4.5. Осуществить разбиение **D(q)** на эквивалентные классы так, чтобы в один класс попадали полномочия (элементы **D(q)**), когда они специфицируют один и тот же ресурс r из набора **R'.**

В каждом классе произвести операцию логического **ИЛИ** элементов **D(q)** с учетом типа операции **e.**

В результате формируется новый набор полномочий на каждую единицу ресурса, указанного в **D(q)** - F(**u, q**). Набор F(**u, q**) называется фактической привилегией пользователя **u** по отношению к запросу **q.**

4.6. Вычислить условие фактического доступа **(EAC),** соответствующее запросу **q**, через операции логического **ИЛИ** по элементам полномочий F(**u, q**) и запрашиваемым ресурсам **r** из набора **R'**, и получить тем самым набор **R''** – набор фактически доступных по запросу ресурсов.

4.7. Оценить **EAC** и принять решение о доступе:

- разрешить доступ, если **R''** и **R'** полностью перекрываются;
- отказать в доступе в противном случае.

Заметим, что при всей своей наглядности модель Хартсона обладает одним, но существенным недостатком – безопасность системы на основе данной модели строго не доказана. Пользователи, осуществляя законный доступ к ресурсам, могут изменять состояния системы, в том числе, изменять множество ресурсов R. Тем самым может изменяться и сама область безопасности. Сохранится ли в таком случае безопасность системы? Модель ответа на данный вопрос не дает.

2.1.2. Модели на основе матрицы доступа

В теоретическом и практическом плане наибольшее развитие и применение получили дискреционные модели, основанные на матрице доступа. В данных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы объектам доступа, а в ячейках записываются разрешенные операции соответствующего субъекта над соответствующим объектом – см. рис. 2.1.

Рис. 2.1. Матрица доступа

«Прописанные» в ячейках матрицы права доступа в виде разрешенных операций над объектами определяют виды безопасных доступов соответствующего субъекта к соответствующему объекту. Для выражения типов разрешенных операций используются специальные обозначения, составляющие основу (алфавит) некоторого языка описания политики разграничения доступа – см. рис. 2.1. Таким образом, в рамках дискреционной политики каждая ячейка агрегирует некоторое подмножество троек «субъект-операция(поток)-объект».

В соответствии с аксиомой 1.3.3 матрица доступа представляет ассоциированный с монитором безопасности объект, содержащий информацию по политике разграничения доступа в конкретной системе. Соответственно, принцип (структура) организации, размещение, а также процессы создания, изменения матрицы доступа определяются конкретными моделями и конкретными программно-техническими решениями КС, в которых они реализуются.

По принципу организации матрицы доступа в реальных системах используются два подхода – централизованный и распределенный.

При централизованном подходе матрица доступа создается как отдельный самостоятельный объект с особым порядком размещения и доступа к нему. Количество объектов доступа и порождаемых пользователями субъектов доступа в реальных КС может достигать очень больших величин, и, кроме того, подвержено динамическому изменению. Поэтому при централизованном подходе в большинстве систем строки матрицы доступа характеризуют не субъектов, а непосредственно самих пользователей и их группы, зарегистрированные для работы в системе. Для уменьшения количества столбцов матрицы, объекты доступа КС могут агрегироваться в две группы – группу объектов, доступ к которым не ограничен (т. е. разрешен любым пользователям по любым операциям), и группу объектов собственно дискреционного (избирательно разграничительного) доступа. Соответственно, в матрице доступа представляются права пользователей только к объектам второй группы, что позволяет существенно уменьшить ее размерность. Наличие или создание в матрице доступа столбца (строки) для какого-либо объекта фактически означает его регистрацию в системе в качестве объекта дискреционного доступа с соответствующими правами соответствующих пользователей. Наиболее характерным и известным примером такого подхода являются т. н. «биты доступа» в UNIX-системах.

При распределенном подходе матрица доступа как отдельный объект не создается, а представляется или так называемыми «списками доступа», распределенными по объектам системы, или так называемыми «списками возможностей», распределенными по субъектам доступа. В первом случае каждый объект системы, помимо идентифицирующих характеристик, наделяется еще своеобразной биркой, непосредственно связанной с самим объектом, и представляющей, по сути, соответствующий столбец матрицы доступа. Во втором случае своеобразную бирку с перечнем разрешенных для доступа объектов (по сути, строку матрицы доступа) получает каждый субъект при своей

инициализации. Добавим также, что через «списки возможностей» (маркеры доступа) субъектов реализуется широко используемый на практике механизм привилегий, наделяющий субъектов правами выполнять определенные операции над всеми объектами или их определенными группами (типами объектов), что формирует дополнительные аспекты дискреционной политики разграничения доступа.

И централизованный, и распределенный принцип организации матрицы доступа имеет свои преимущества и недостатки, присущие в целом централизованному и децентрализованному принципам организации и управления.

По механизму создания и изменения матрицы доступа, т. е. фактически по принципу управления доступом, выделяются также два подхода:

• принудительное управление доступом;

• добровольное управление доступом.

Принцип принудительного управления доступом основывается на парадигме доверенных субъектов и непосредственно вытекает из следствия 1.3.3 аксиомы 1.3.3 по созданию и функционированию защищенных систем. Согласно принудительному способу право создания и изменения матрицы доступа имеют только субъекты администратора системы, который при регистрации для работы в системе нового пользователя создает с соответствующим заполнением новую строку матрицы доступа, а при возникновении нового объекта, подлежащего избирательному доступу, образует новый столбец матрицы доступа.

Нетрудно видеть, что такой способ приемлем только при фиксированном или ограниченном количестве объектов доступа или, требует агрегирования объектов доступа в определенные группы и перехода к управлению правами доступа по группам (типам) объектов доступа. Подобный подход наиболее широко представлен в базах данных, где управление доступом в большинстве случаев осуществляется на уровне логических информационных объектов (в реляционных СУБД – таблицы), представляющих

агрегирование однотипных элементарных объектов доступа – записей (в реляционных СУБД – кортежи, т. е. табличные строки).

Принцип добровольного управления доступом основывается на парадигме «владения» объектами.

Определение 2.1.1. Владельцем объекта доступа называется пользователь, инициализировавший поток, в результате которого объект возник в системе, или определенный владельцем иным образом (получивший право владения объектом).

Тем самым, в дополнение к основным положениям субъектно- объектной модели вводится специальное отображение множества объектов на множество субъектов доступа, называемое владением, ставящее в каждый фиксированный момент времени каждому объекту системы подмножество субъектов доступа, инициализированных пользователем- владельцем объекта.

Добровольное управление доступом выражается следующим правилом:

Правило 2.1.1. Права доступа к объекту определяют (устанавливают) их владельцы.

Из данного правила следует, что заполнение и изменение ячеек матрицы доступа осуществляют субъекты пользователей-владельцев соответствующих объектов.

Нетрудно видеть, что подобный подход обеспечивает управление доступом в тех системах, в которых количество объектов доступа является значительным или неопределенным, так как переносит процесс управления на владельцев объектов, мощность подмножества объектов управления, для которых в большинстве случаев существенно меньше общей мощности множества объектов в системе. Такая ситуация наиболее характерна для операционных систем.

Во многих КС право владения объектом его прежним владельцем может быть передано другому пользователю. Кроме того, как уже отмечалось, в ОС, составляющих основу любых КС, декомпозиция системы на субъекты и объекты может меняться в различные моменты времени (в результате операций создания, копирования, переименования и удаления объектов, с одной стороны, а с другой, в результате инициализации и прекращения функционирования пользователями субъектов доступа). В результате матрица доступа имеет динамический характер (появляются или уничтожаются строки, или столбцы, изменяется содержимое ячеек). Поэтому права доступа в таких системах могут «гулять», распространяться по субъектам системы. В этом случае возникает проблема самого понятия безопасности в смысле главного метода ее обеспечения – разграничения доступа, и требуется исследование условий и процессов распространения прав доступа.

В теоретическом плане впервые данная проблема была исследована Харрисоном, Руззо и Ульманом, которые для этого разработали специальную формальную модель дискреционного доступа, называемую по их имени, или сокращенно модель **HRU**. Основные положения модели рассматриваются в следующем параграфе.

2.1.3. Модели распространения прав доступа

В моделях распространения прав доступа проблема безопасности КС рассматривается с точки зрения анализа возможности или невозможности получения каким-либо субъектом определенных прав доступа к определенному объекту. Иначе говоря, анализируются, прежде всего, изменения прав доступа субъектов к объектам в результате некоторых обусловленных операций (переходов), а не сами процессы осуществления доступов субъектов к объектам.

2.1.3.1. Модель Харисона-Руззо-Ульмана (HRU-модель)

Основные положения модели сводятся к следующему.

1. КС представляется тройкой сущностей:

- множеством исходных объектов $\boldsymbol{O}\,(\boldsymbol{o}_1, \boldsymbol{o}_2, \ldots, \boldsymbol{o}_M)$;

- множеством исходных субъектов $\boldsymbol{S}\ (\boldsymbol{s}_1, \boldsymbol{s}_2, \ \ldots, \ \boldsymbol{s}_N)$, при этом $\mathbf{S} \subseteq \mathbf{O}$;

- матрицей доступа **A**, каждая ячейка которой специфицирует права доступа к объектам из конечного набора прав доступа **R**

$$(\boldsymbol{r}_1, \boldsymbol{r}_2, \ \ldots, \ \boldsymbol{r}_K),\ \text{т. е.}\ \mathbf{A}[\boldsymbol{s}, \boldsymbol{o}] \subseteq \boldsymbol{R}.$$

Права доступа $\boldsymbol{r}_i$, размещаемые в ячейках матрицы доступа **A[s,o],** определяют совокупность допустимых (разрешенных) операций над объектом из полного набора возможных операций над объектами.

Заметим также, что модель **HRU** несколько отличается от рассмотренной в п. 1.3.2 субъектно-объектной модели КС, представляя субъектов доступа «активизированными» состояниями некоторого подмножества объектов системы (т. е. $\mathbf{S} \subseteq \mathbf{O}$), что, с одной стороны, огрубляет саму суть субъектов доступа, но, с другой стороны позволяет ввести понятие доступа субъекта к субъекту.

2. Функционирование системы рассматривается исключительно с точки зрения изменений в матрице доступа. Возможные изменения определяются шестью примитивными операторами **Op**:

- Enter **r** into **A[s,o]** – ввести право r в ячейку **A[s,o]**;

- Delete **r** from **A[s,o]** – удалить право r из ячейки **A[s,o]**;

- Create subject **s** – создать субъект s (т. е. новую строку матрицы **A**);

- Create object **o** – создать объект o (т. е. новый столбец матрицы **A**);

- Destroy subject **s** – уничтожить субъект s;

- Destroy object **o** – уничтожить объект o.

В результате выполнения примитивного оператора осуществляется переход КС из состояния **Q = (S, O, A)** в новое состояние **Q'= (S', O', A').**

В табл. 2.1 приведены условия и особенности изменения состояния системы под воздействием примитивных операторов.

3. Состояния системы изменяются под воздействием запросов на модификацию матрицы доступа в виде команд следующего формата:

Command $\alpha(x_1, x_2, \ldots, x_k)$
if r_1 *in* $\mathbf{A}[x_{S_1}, x_{O_1}]$ *and* (условия выполнения команды)
r_2 *in* $\mathbf{A}[x_{S_2}, x_{O_2}]$ *and*
.
.
.
r_m *in* $\mathbf{A}[x_{S_m}, x_{O_m}]$
then (операторы, составляющие команды)
$op_1, op_2, \ldots, op_n$

Каждое состояние системы $\mathbf{Q}_i$ является результатом выполнения некоторой команды α_l, применимой по ее условиям к предыдущему состоянию $\mathbf{Q}_{i-1}$

$$\mathbf{Q}_i = \alpha_l(\mathbf{Q}_{i-1}),$$

и определяет отношения доступа, которые существуют между сущностями системы в виде множества субъектов, объектов и матрицы прав доступа.

Таблица 2.1

Условия и особенности изменения состояния системы под воздействием примитивных операторов

Примитивный оператор модели **HRU**	Условия выполнения	Новое состояние системы
Enter **r** *into* **A**[**s**,**o**]	$s \in S$, $o \in O$	$S'=S$, $O'=O$, $A'[s, o] = A[s, o] \cup \{r\}$, если $(s',o') \neq (s,o) \Rightarrow A'[s',o']=A[s,o]$
Delete **r** *from* **A**[**s**,**o**]	$s \in S$, $o \in O$	$S'=S$, $O'=O$, $A'[s,o]= A[s,o] \setminus \{r\}$, если $(s',o') \neq (s,o) \Rightarrow A'[s',o']=A[s,o]$
Create subject s'	$s' \notin S$	$S'=S \cup \{s'\}$, $O'=O \cup \{s'\}$, если $(s,o) \in S \times O \Rightarrow A'[s,o]=A[s,o]$, если $o \in O' \Rightarrow A'[s',o] = \varnothing$, если $s \in S' \Rightarrow A'[s, s'] = \varnothing$
Create object o'	$o' \notin O$	$S'= S$, $O'=O \cup \{o'\}$, если $(s,o) \in S \times O \Rightarrow A'[s,o]=A[s,o]$, если $s \in S' \Rightarrow A'[s,o] = \varnothing$
Destroy subject s'	$s' \in S$	$S'=S \setminus \{s'\}$, $O'=O \setminus \{s'\}$, если $(s,o) \in S' \times O' \Rightarrow A'[s,o]=A[s,o]$
Destroy object o'	$o' \in O \setminus S$	$S'=S$, $O'=O \setminus \{o'\}$,
		если $(s,o) \in S' \times O' \Rightarrow A'[s,o]=A[s,o]$

4. Безопасность системы определяется некоторыми условиями на начальное состояние системы Q_0, а также особенностями системы команд **α**. Формулируется следующий критерий безопасности:

Определение 2.1.2. (Критерий безопасности в модели HRU). Система является безопасной относительно права **r**, если для заданного начального состояния $Q_0 = (S_0, O_0, A_0)$ не существует применимой к Q_0 последовательности команд, в результате которой право **r** будет занесено в ячейку матрицы **A[s,o]**, в которой оно отсутствовало в начальном состоянии Q_0 .

Действительно из самого понятия разграничения доступа вытекает необходимость наложения ограничений на определенные отношения доступа (определенных субъектов к определенным объектам по определенным операциям). Очевидно, что безопасность (состояние защищенности информации) в системе, заключается в том, чтобы эти ограничения соблюдались все время функционирования системы, и, в том числе, в начальном состоянии Q_0. Иначе говоря, в неформальном выражении безопасность системы будет определяться тем, возможно или нет в процессе функционирования системы получение некоторым субъектом определенного права доступа к некоторому объекту, которым он изначально (т. е. в начальном состоянии Q_0) не обладал.

Для рассмотрения условий, при которых выполняется данный критерий, вводится понятие монооперационных систем.

Определение 2.1.3. Система называется монооперационной, если каждая команда **α** выполняет один примитивный оператор op_i.

Авторы модели **HRU** представили следующие теоремы, доказательство которых не приводится ввиду их громоздкости и доступности в литературе.

Теорема 2.1.1**.** Существует алгоритм, который проверяет, является ли исходное состояние монооперационной системы безопасным для данного права **r.**

Из теоремы 2.1.1 следует, что проблема безопасности может быть решена для монооперационных систем. К сожалению, теорема доказывает только само существование проверяющего алгоритма, но не дает каких- либо рекомендаций или других оснований для его разработки и построения.

Харрисон, Руззо и Ульман показали также, что безопасными могут быть монотонные системы (не содержащие

операций Delete и Destroy), системы, не содержащие операций Create, и моно-условные системы (в которых запросы содержат только одно условие). Вместе с тем, все подобные системы существенно ограничены в функциональности.

Теорема 2.1.2. Задача определения безопасности для данного права r в системах с запросами произвольного вида является алгоритмически неразрешимой.

Говоря иными словами, теорема 2.1.2 утверждает, что поведение систем на основе модели **HRU** с точки зрения безопасности является непредсказуемым.

Помимо проблем с неопределенностью распространения прав доступа в системах на основе модели HRU была подмечена еще одна серьезная проблема – отсутствие контроля за порождением потоков информации, и, в частности, контроля за порождением субъектов, следствием чего могут быть так называемые «троянские» программы. В модели HRU «правильность», легитимность инициируемых из объектов-источников субъектов доступа никак не контролируется. В результате, злоумышленник в системе может осуществить неправомерный доступ к информации на основе подмены свойств субъектов доступа.

Данные результаты, опубликованные в середине 70-х годов, вызвали обескураживающий эффект среди исследователей теории компьютерной безопасности, но, вместе с тем, стимулировали поиски других подходов к обеспечению проблемы безопасности.

В частности, для смягчения условий, в которых можно производить формальное доказательство безопасности, а также для введения контроля за порождением объектов была предложена модель «типизованной матрицы доступа» (модель Type Access Matrix – **TAM**).

2.1.3.2. Модель типизованной матрицы доступа

1. КС представляется четверкой сущностей:

- множеством исходных объектов $O\,(o_1,\ o_2,\ \ldots,\ o_M)$;

- множеством исходных субъектов $S\ (s_1,\ s_2,\ \ldots,\ s_N)$, при этом

$$\mathbf{S \subseteq O};$$

- матрицей доступа **A**, каждая ячейка которой специфицирует права доступа к объектам из конечного набора прав доступа $R\,(r_1,\ r_2,\ \ldots,\ r_K)$, т. е. **A[s,o] ⊆ R**;

- множеством (конечным набором) типов безопасности **T** $(t_1,\ t_2,\ldots,\ t_L)$ с одним из которых создается любой объект, (включая
субъекты). Тип объекта впоследствии не меняется (т. н. сильная организация типов). Таким образом, в системе задана функция $f_t: O \to T$, ставящая в соответствие каждому объекту некоторый тип.

2. Вводятся примитивные операторы, изменяющие состояние матрицы доступа с учетом типизации объектов (объектов и субъектов доступа):

- Enter **r** into **A[s,o]** – ввести право **r** в ячейку **A[s,o];**
- Delete **r** from **A[s,o]** – удалить право **r** из ячейки **A[s,o]**;
- Create subject **s** of type **t** – создать субъект **s** типа **t**;
- Create object **o** of type **t** – создать объект **o** типа **t**;
- Destroy subject **s** – уничтожить субъект **s**;
- Destroy object **o** – уничтожить объект **o**.

В результате выполнения примитивного оператора осуществляется переход КС из состояния **Q = (S, O, A)** в новое состояние **Q'= (S', O', A').**

В табл. 2.2 приведены условия и особенности изменения состояния системы под воздействием примитивных операторов с учетом типизации объектов.

Таблица 2.2

Условия и особенности изменения состояния системы
под воздействием примитивных операторов
с учетом типизации объектов

Примитивный оператор модели ТАМ	Условия выполнения	Новое состояние системы
Enter r *into* $A[s,o]$	$s \in S$, $o \in O$	$S'=S$, $O'=O$, $\forall o \in O \quad f_t'(o)=f_t(o)$, $A'[s,o]=A[s,o] \cup \{r\}$, если $(s',o') \neq (s,o) \Rightarrow A'[s',o']=A[s,o]$
Delete r *from* $A[s,o]$	$s \in S$, $o \in O$	$S'=S$, $O'=O$, $\forall o \in O \quad f_t'(o)=f_t(o)$, $A'[s,o]= A[s,o] \setminus \{r\}$, если $(s',o') \neq (s,o) \Rightarrow A'[s',o']=A[s,o]$
Create subject s' *of type* t_s	$s' \notin S$	$S'=S \cup \{s'\}$, $O'=O \cup \{s'\}$, $f_t'(s')=t_s$, $\forall o \in O \quad f_t'(o)=f_t(o)$, если $(s,o) \in S \times O \Rightarrow A'[s,o]=A[s,o]$, если $o \in O' \Rightarrow A'[s',o] = \varnothing$, если $s \in S' \Rightarrow A'[s,s'] = \varnothing$
Create object o' *of type* t_o	$o' \notin O$	$S'=S$, $O'=O \cup \{o'\}$, $f_t'(o')=t_o$, $\forall o \in O \quad f_t'(o)=f_t(o)$ если $(s,o) \in S \times O \Rightarrow A'[s,o]=A[s,o]$, если $s \in S' \Rightarrow A'[s,o] = \varnothing$
Destroy subject s'	$s' \in S$	$S'=S \setminus \{s'\}$, $O'=O \setminus \{s'\}$, $\forall o \in O \; f_t'(o)=f_t(o)$, $f_t'(s')=$ не определено если $(s,o) \in S' \times O' \Rightarrow A'[s,o]=A[s,o]$
Destroy object o'	$o' \in O \setminus S$	$S'=S$, $O'=O \setminus \{o'\}$, $\forall o \in O' \; f_t'(o)=f_t(o)$, $f_t'(o')=$не определено если $(s,o) \in S' \times O' \Rightarrow A'[s,o]=A[s,o]$

3. Состояния системы так же, как и в модели HRU, изменяются под воздействием запросов на модификацию матрицы доступа в виде команд, формат которых с учетом типизованного характера объектов системы имеет следующий вид:

Command $\alpha(x_1{:}t_1,\ x_2{:}t_2,\ \ldots,\ x_k{:}t_k)$

if r_1 *in* $\mathbf{A}[x_{S_1},\ x_{O_1}]$ *and* (условия выполнения команды)

r_2 *in* $\mathbf{A}[x_{S_2},\ x_{O_2}]$ *and*

.

.

.

r_m *in* $\mathbf{A}[x_{S_m},\ x_{O_m}]$

then

$op_1, op_2, \ldots, op_n$ (операторы, составляющие команду).

Таким образом, при выполнении команд на модификацию матрицы доступа вводится контроль типов фактических параметров команды, т. е. контроль типов объектов и субъектов, задействованных в условиях выполнения команды. На этой основе можно сформулировать ограничения, накладываемые на команды, при которых могут быть смягчены условия безопасности системы.

Для формулирования ограничений на запросы команд перехода в новое состояние системы определяются отношения между типами, в частности, понятие дочернего и родительского типа.

Определение 2.1.4. Тип t_i является дочерним типом в команде **α**, если в теле **α** имеет место один из следующих элементарных операторов: «Create subject **s'** of type t_i» или «Create object o' of type t_i». В противном случае тип t_i является родительским типом.

Основываясь на понятии родительских и дочерних типов, можно описать взаимосвязи между различными типами с помощью графа отношений «наследственности» при операциях порождения сущностей (субъектов и объектов). Такой граф является ориентированным (орграфом) и называется «графом создания». Множество вершин графа образуется множеством типов безопасности Т. Ребро от

вершины t_i к вершине t_j в графе имеется тогда и только тогда, когда существует команда **α**, в которой тип t_i является родительским, а тип t_j дочерним.

Также, как и в модели **HRU**, используется понятие монотонной **(MTAM)** системы, которая не содержит примитивных операторов **Delete** и **Destroy**.

Определение 2.1.5. Реализация **MTAM** является ацикличной тогда и только тогда, когда ее граф создания не содержит циклов.

Мы видим, что критерий безопасности Хариссона-Руззо-Ульмана (определение 2.1.2) разрешим для ациклических реализаций системы с монотонной **TAM**, а требование одноусловности можно заменить требованием ацикличности графа создания системы. Требование ацикличности с формальной точки зрения позволяет существенно сократить и ограничить количество путей на графе создания при рассмотрении и доказательстве безопасности в системе. С неформальной точки зрения ацикличность означает, что последовательность состояний системы должна следовать определенному маршруту на графе создания, так как возникновению новых сущностей в системе должно предшествовать наличие объектов определенных родительских типов. В результате поведение системы становится более предсказуемым.

Кроме того, на основе специальной системы типов (например, типы «файл», «программа» для объектов; «user», «administrator», «auditor» для субъектов) в КС на основе **TAM** возможна организация эффективного контроля за порождением субъектов с нейтрализацией проблемы «троянских» программ.

2.1.3.3. Модель TAKE-GRANT

Еще одной моделью, имеющей важное теоретическое значение в исследовании процессов распространения прав доступа в системах, основанных на политике дискреционного

доступа, является модель **TAKE-GRANT**, представленная Джонсом, Липтоном и Шнайдером в 1976 г.

Модель **TAKE-GRANT**, отталкиваясь от основных положений субъектно-объектной модели КС, использует аппарат теории графов для моделирования системы разграничения доступа и процессов ее изменения.

Основные положения модели сводятся к следующему.

1. КС рассматривается как граф **Г (O, S, E)**, в котором множество вершин представлено (см. рис. 2.2):

- множеством объектов **O** доступа;

- множеством субъектов **S** доступа, причем **S ⊆ O**, а множество ребер:

- множеством **E** установленных прав доступа (x, y, α) субъекта x к объекту y с правом α из конечного набора прав $\alpha \subseteq \boldsymbol{R}\,(r_1, r_2, \ldots, r_K) \cup \{t, g\}$, в том числе с двумя специфическими правами – правом **take** (t – право брать права доступа у какого-либо объекта по отношению к другому объекту) и правом **grant** (g – право предоставлять права доступа к определенному объекту другому субъекту).

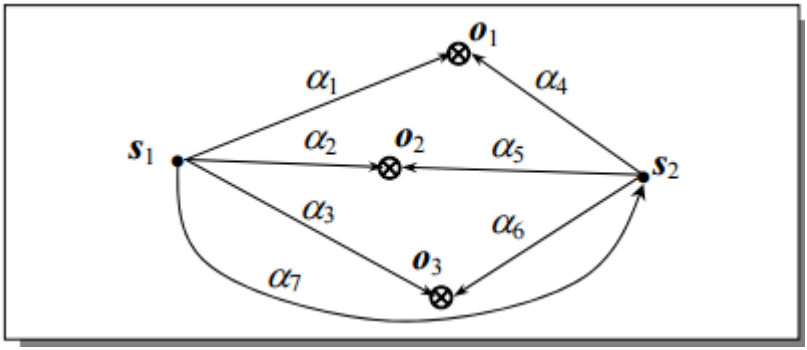

Рис. 2.2. Граф доступов **Г** в модели **TAKE-GRANT**
(обозначения: • – вершины, соответствующие субъектам,
⊗ – вершины, соответствующие объектам доступа,
$\alpha_1 \subseteq \mathbf{R}$ – права доступа)

Как и в модели **HRU**, субъекты рассматриваются в качестве активизированного состояния некоторых объектов, и поэтому граф **Г** не является двудольным, так как могут существовать дуги (права доступа) между субъектами.

2. Состояния КС (т. е. состояние системы разграничения доступа) изменяются под воздействием команд 4-х видов.

2.1. Команда **«Брать»** – **take**(α, x, y, z) – см. рис. 2.3.

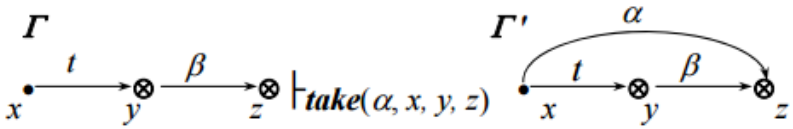

Рис. 2.3. Изменение состояния фрагмента графа доступов **Г** по команде **«Брать»** – субъект x берет права доступа α ⊆ β на объект z у объекта y (обозначения: ⊢**c** – переход графа **Г** в новое состояние **Г '** по команде **c**; x∈ **S**; y, z∈ **O**)

2.2. Команда **«Давать»** – **grant**(α, x, y, z) – см. рис. 2.4.

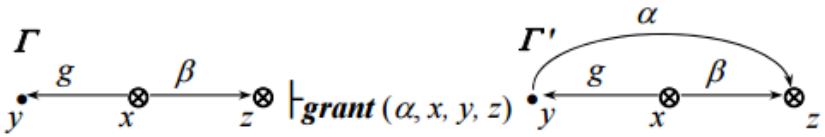

Рис. 2.4. Субъект x дает объекту y право α ⊆ β на доступ к объекту

2.3. Команда **«Создать»** – **create**(β, x, y) – см. рис. 2.5.

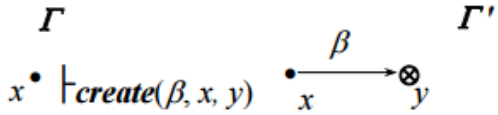

Рис. 2.5. Субъект x создает объект y с правами доступа на него β ⊆ **R** (y – новый объект, **O**'=**O** ∪{y})

2.4. Команда **«Удалить»** – **remove**(α, x, y) – см. рис. 2.6.

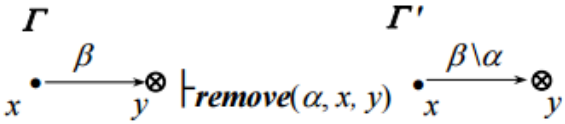

Рис. 2.6. Субъект x удаляет права доступа α ⊆ β на объект y

В табл. 2.3 приведены условия и особенности изменения состояния системы под воздействием представленных выше команд.

Таблица 2.3

Условия и особенности изменения состояния системы под воздействием команд

Команда модели TAKE-GRANT	Условия выполнения	Новое состояние системы
take(α, x, y, z)	$x \in \boldsymbol{S}$, $(x, y, t) \in \boldsymbol{E}$, $(y, z, \beta)^1 \in \boldsymbol{E}$ $x \neq z$, $\alpha \subseteq \beta$	$\boldsymbol{S'}=\boldsymbol{S}$, $\boldsymbol{O'}=\boldsymbol{O}$, $\boldsymbol{E}=\boldsymbol{E'} \cup \{(x, z, \alpha)\}$
grant(α,x,y, z)	$x \in \boldsymbol{S}$, $(x, y, g) \in \boldsymbol{E}$, $(y, z, \beta) \in \boldsymbol{E}$ $x \neq z$, $\alpha \subseteq \beta$	$\boldsymbol{S'}=\boldsymbol{S}$, $\boldsymbol{O'}=\boldsymbol{O}$, $\boldsymbol{E}=\boldsymbol{E'} \cup \{(y, z, \alpha)\}$
create(β, x, y)	$x \in \boldsymbol{S}$, $y \notin \boldsymbol{O}$	$\boldsymbol{O'}=\boldsymbol{O} \cup \{y\}$, $\boldsymbol{S'}=\boldsymbol{S} \cup \{y\}$, если y – субъект $\boldsymbol{E}=\boldsymbol{E'} \cup \{(y, z, \beta)\}$
remove(α,x,y)	$x \in \boldsymbol{S}$, $y \in \boldsymbol{O}$, $(x, y, \beta) \in \boldsymbol{E}$, $\alpha \subseteq \beta$	$\boldsymbol{S'}=\boldsymbol{S}$, $\boldsymbol{O'}=\boldsymbol{O}$, $\boldsymbol{E}=\boldsymbol{E'} \setminus \{(x,y,\alpha)\} \cup \{(x, y, \beta)\}$

3. Безопасность системы рассматривается с точки зрения возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии $\boldsymbol{\Gamma}_0(\boldsymbol{O}_0, \boldsymbol{S}_0, \boldsymbol{E}_0)$ такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения команд, представленных в

табл. 2.3. Предметом анализа при этом являются установленные в начальный момент времени отношения между субъекта- ми по получению и передаче прав доступа на объекты системы, а также возможные ограничения на дальнейшую кооперацию субъектов в процессе функционирования системы. Рассматриваются два возможных варианта:

- санкционированное получение прав доступа (безопасное функционирование системы);
- похищение прав доступа (условия, в которых безопасность не обеспечивается).

3.1. *Санкционированное получение прав доступа*

Вводятся следующие определения.

Определение 2.1.6. Для исходного состояния систем $\Gamma_0(O_0, S_0, E_0)$ и прав доступа $\alpha \subseteq R$ предикат «возможен доступ (α, x, y, Γ_0)» является истинным тогда и только тогда, когда существуют графы доступов системы $\Gamma_1(O_1, S_1, E_1)$, $\Gamma_2(O_2, S_2, E_2)$, …, $\Gamma_N(O_N, S_N, E_N)$, такие, что:

$\Gamma_0(O_0,S_0,E_0) \vdash_{c_1} \Gamma_1(O_1,S_1,E_1) \vdash_{c_2} \dots \vdash_{c_N} \Gamma_N(O_N,S_N,E_N)$ и $(x, y, \alpha) \in E_N$

где c_1, c_2, …, c_N – команды вида 2.1, 2.2, 2.3 и 2.4.

Говоря иначе, доступ субъекта x к объекту y с правом $\alpha \subseteq \mathbf{R}$, отсутствующий в начальном состоянии системы $(x, y, \alpha) \notin E_0$, возможен тогда и только тогда, когда существует последовательность перехода системы из состояния в состояние $(\Gamma_0, \Gamma_1, \dots, \Gamma_N)$ под воздействием команд 2.1, 2.2, 2.3 и 2.4.

Определение 2.1.7. Вершины графа доступов являются tg-связными (соединены tg-путем), если в графе между ними существует такой путь, что каждая дуга этого пути выражает право t или g (без учета направления дуг).

Вершины непосредственно tg-связаны, если tg-путь между ними состоит из единственной дуги.

Справедлива следующая теорема.

Теорема 2.1.3. В графе доступов $\Gamma_0(O_0, S_0, E_0)$, содержащем только вершины-субъекты, предикат «возможен доступ(α, x, y, Γ_0)» истинен тогда и только тогда, когда выполняются следующие условия:

Условие 2.1.3.1. Существуют субъекты $s_1, \ldots, s_m$ такие, что $(s_i, y, \gamma_i) \in E_0$ для i=1, …, m и $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$.

Условие 2.1.3.2. Субъект x соединен в графе Γ_0 tg-путем с каждым субъектом s_i для i=1, …, m.

Определение 2.1.8. Островом в произвольном графе доступов **Г** называется его максимальный tg-связный подграф, состоящий только из вершин субъектов.

Заметим, что остров, по сути, характеризует некую группу субъектов, кооперация которых в правах доступа не ограничена и процессы получения доступа внутри группы описываются теоремой 2.3.

Определение 2.1.9. Мостом в графе доступов Г называется tg–путь, концами которого являются вершины-субъекты; при этом словарная запись tg-пути должна иметь вид $\vec{t}^*, \vec{t}^* g \vec{t}^*, \vec{t}^* g \vec{t}^*$, , где символ * означает многократное (в том числе нулевое) повторение.

Определение 2.1.10. Начальным пролетом моста в графе доступов **Г** называется tg-путь, началом которого является вершина-субъект; при этом словарная запись tg-пути должна иметь вид $\vec{t}^* g$.

Определение 2.1.11. Конечным пролетом моста в графе доступов Г называется tg-путь, началом которого является вершина-субъект; при этом словарная запись tg-пути должна иметь вид $\vec{t}^*$.

Справедлива следующая теорема.

Теорема 2.1.4. В произвольном графе доступов $\Gamma_0(O_0, S_0, E_0)$ предикат «возможен доступ(α, x, y, Γ_0)» истинен тогда и только тогда, когда выполняются условия 2.1.4.1, 2.1.4.2 и 2.1.4.3:

Условие 2.1.4.1. Существуют объекты $s_1,\dots,s_m$ такие, что $(s_i, y, \gamma_i)\in E_0$ для i=1, …, m и $\alpha=\gamma_1\cup\dots\cup\gamma_m$.

Условие 2.1.4.2. Существуют вершины-субъекты $x_1',\dots,x_m'$ и $s_1',\dots,s_m'$ такие, что:

- $x=x_i'$ или x_i' соединен с x начальным пролетом моста для i=1, …, m;
- $s_i=s_i'$ или s_i' соединен с s_i конечным пролетом моста для i=1, … , m.

Условие 2.1.4.3. Для каждой пары (x_i', s_i'), i=1,…,m, существуют острова $I_{i1},\dots,I_{iu_i}$, $u_i\geq 1$, такие, что $x_i'\in I_{i1}$, $s_i'\in I_{iu_i}$, и мосты между островами I_{ij} и I_{ij+1}.

3.2. Похищение прав доступа

Пусть x, y ∈ O_0 – различные объекты графа доступа $\Gamma_0(O_0, S_0, E_0)$.

Определение 2.1.12. Для исходного состояния системы $\Gamma_0(O_0, S_0, E_0)$ и прав доступа α ⊆ **R** предикат «возможно похищение(α, x, y, Γ_0)» является истинным тогда и только тогда, когда существуют графы доступов системы $\Gamma_1(O_1, S_1, E_1)$, $\Gamma_1(O_2, S_2, E_2)$, …, $\Gamma_N(O_N, S_N, E_N)$ такие, что:
$\Gamma_0(O_0,S_0,E_0)\vdash_{c_1}\Gamma_1(O_1,S_1,E_1)\vdash_{c_2}\dots\vdash_{c_N}\Gamma_N(O_N,S_N,E_N)$ и $(x, y,\alpha)\in E_N$
где c_1, c_2, …, c_N – команды вида 2.1, 2.2, 2.3 и 2.4.

При этом, если ∃ (s, y, α) ∈ O_0, то ∀ z ∈ S_j , j=0,1,…, N выполняется: $c_1\neq$ **grant**(α, s, z, y).

Говоря иначе, согласно определению 2.1.11 похищением прав является процесс получения прав доступа на какой-либо

объект без предоставления прав третьим субъектам со стороны субъекта, обладающего в начальном состоянии требуемыми правами на объект «интереса».

Справедлива следующая теорема.

Теорема 2.1.5. В произвольном графе доступов $\Gamma_0(O_0, S_0, E_0)$ предикат «возможно похищение(α, x, y, Γ_0)» истинен тогда и только тогда, когда выполняются условия 2.1.5.1, 2.1.5.2 и 2.1.5.3:

Условие 2.1.5.1. (x, y,α) $\notin E_0$.

Условие 2.1.5.2. Существуют субъекты $s_1,\ldots,s_m$ такие, что $(s_i, y, \gamma_i) \in E_0$ для i=1, …, m и $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$.

Условие 2.1.5.3. Являются истинными предикаты «возможен доступ (t, x, s_i , Γ_0)» для i=1, …, m.

Отметим, что теорема 2.1.5 также выражает интуитивно понятную ситуацию – если политика разграничения доступа в КС запрещает субъектам, имеющим в исходном состоянии права доступа к определенным объектам, непосредственно предоставлять эти права другим субъектам, которые изначально такими правами не обладают, то, тем не менее, такие первоначально «обделенные» субъекты могут получить данные права при наличии в графе доступов возможностей получения доступа с правом t к первым субъектам.

Таким образом, модель **TAKE-GRANT** играет важную методологическую роль, предоставляя теоретико-графовый инструмент анализа систем разграничения доступа с точки зрения санкционированного и несанкционированного со стороны определенных субъектов распространения прав доступа в рамках дискреционной политики.

2.1.3.4. Расширенная модель TAKE-GRANT

Выразительные методологические возможности модели **TAKE-GRANT** позволили на ее основе разработать расширенную модель **TAKE-GRANT**, играющую важную роль в исследовании возможностей неявных информационных потоков в дискреционных системах разграничения доступа.

Введем следующее определение.

Определение 2.1.13. Неявным информационным потоком между объектами системы называется процесс переноса информации между ними без их непосредственного взаимодействия.

Наиболее простым и наглядным примером неявного информационного потока является наличие общего буфера (объекта с правом доступа к нему **Read**, **Write**) у двух субъектов. Тогда один из субъектов, просматривая (читая) информацию в буфере, может искать и находить информацию из объектов, которые доступны другому пользователю, и информация из которых в процессе работы с ними может оказаться в общем буфере или, скажем, в общей мусорной информационной корзине. В результате может существовать поток без непосредственного взаимодействия субъекта с объектом доступа.

Основные положения расширенной модели **TAKE-GRANT** сводятся к следующему.

1. КС рассматривается как граф **Г (O, S, E)**, в котором множество вершин представлено:

- множеством объектов **O** доступа;

- множеством субъектов **S** доступа, причем **S⊆O**, а множество ребер:

- множеством установленных прав доступа (x, y, α) субъекта x к объекту y с правом α из набора прав доступа **R**, включающего всего два вида (методов) доступа – **Read** и **Write**.

2. Для исследования процессов возникновения неявных информационных потоков вводятся шесть команд (операций) преобразования графа доступов, каждая из которых сопровождается порождением мнимой дуги, собственно и отображающей неявный информационный поток между объектами системы:

2.1. Команда (без названия) – см. рис. 2.7.

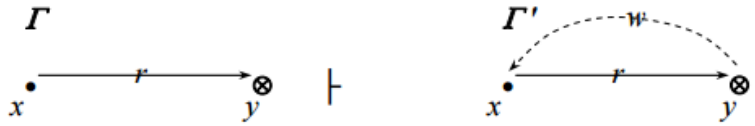

Рис. 2.7. Субъект x получает возможность записи (в себя) информации, осуществляя доступ r к объекту y

2.2. Команда (без названия) – см. рис. 2.8.

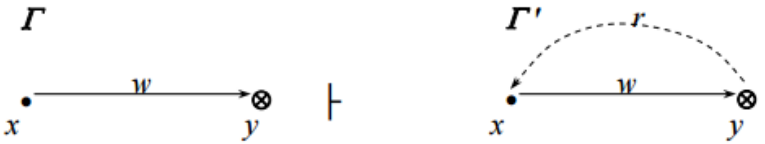

Рис. 2.8. Субъект x получает возможность чтения информации, осуществляя доступ w к объекту y

2.3. Команда **post** (x, y, z) – см. рис. 2.9.

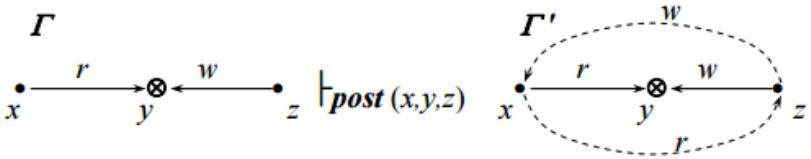

Рис. 2.9. Субъект x получает возможность чтения информации от (из) другого субъекта z, осуществляя доступ r к объекту y, к которому субъект z осуществляет доступ w, а субъект z, в свою очередь, получает возможность записи своей информации в субъект x

2.4. Команда **spy** (x, y, z) – см. рис. 2.10.

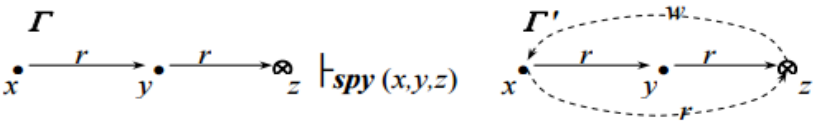

Рис. 2.10. Субъект x получает возможность чтения информации из объекта z, осуществляя доступ r к субъекту y, который, в свою очередь, осуществляет доступ r к объекту z, при этом также у субъекта x возникает возможность записи к себе информации из объекта z

2.5. Команда **find** (x, y, z) – см. рис. 2.11.

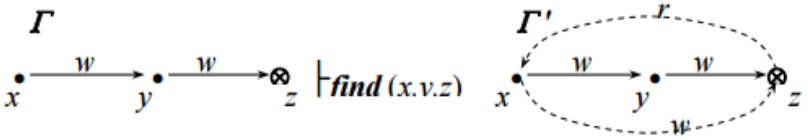

Рис. 2.11. Субъект x получает возможность чтения информации из объекта z, осуществляя доступ w к субъекту y, который, в свою очередь, осуществляет доступ w к объекту z, при этом также у субъекта x возникает возможность записи к себе информации из объекта z

2.6. Команда **pass** (x, y, z) – см. рис. 2.12.

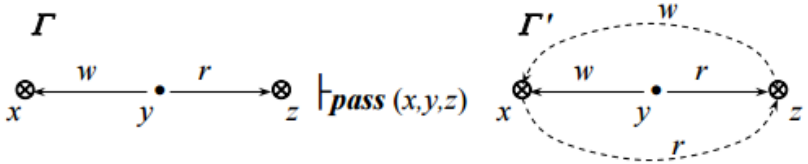

Рис. 2.12. При осуществлении субъектом y доступа r к объекту z возникает возможность внесения из него информации в другой объект x, к которому субъект y осуществляет доступ w, и, кроме того, возникает возможность получения информации (чтения) в объекте x из объекта z

3. Анализ возможности возникновения неявного информационного канала (потока) между двумя произвольными объектами (субъектами) x и y системы осуществляется на основе поиска и построения в графе доступов пути между x и y, образованного мнимыми дугами, порождаемыми применением команд 2.1,…,2.6 к различным фрагментам исходного графа доступов.

Процедуры построения такого пути могут основываться на известных поисковых алгоритмах в графах, в частности, на методах поиска в глубину (ПВГ) и поиска в ширину (ПВШ), широко применяемых в сфере задач дискретной оптимизации. Алгоритмический характер подобных процедур позволяет их легко автоматизировать. Заметим также, что такие процедуры могут приводить к построению не одного, а нескольких путей возможного возникновения неявных информационных потоков. При этом становится возможным анализ и решение, если так можно выразиться, «тонких» задач относительно систем разграничения доступа:

• при допущении справедливости гипотезы, или при наличии достоверных фактов о состоявшемся неявном информационном потоке от одного объекта(субъекта) к другому объекту(субъекту), анализировать и выявлять круг возможных субъектов-«заговорщиков» подобного несанкционированного информационного потока;

• для какой-либо пары объектов (субъектов) осуществлять анализ определенных количественных характеристик возможности неявного информационного потока между ними по тому или иному маршруту.

Решение задач первого вида возможно на основе уже упоминавшихся методов ПВГ и ПВШ на графах. В качестве количественных характеристик в задачах второго вида могут быть выбраны характеристики, выражающие в интервальной или ранговой шкале вероятность возникновения канала в зависимости от количественных параметров (длина пути канала на графе доступов) или качественных параметров (вид канала – сочетанием каких команд «де-факто» и по каким

субъектам образован соответствующий путь на графе доступов).

Возможные каналы неявных информационных потоков определяются конкретным графом доступов КС, который, в свою очередь, отражает установленные для пользователей-субъектов права доступа к объектам системы в рамках принятой политики разграничения доступа. Система разграничения доступа должна обеспечивать доступ пользователей только к тем объектам, которые им необходимы для выполнения функциональных обязанностей или необходимы на основе других соображений. Иначе говоря, структура системы объектов доступа и система разграничения доступа к ним должны быть построены таким образом, чтобы не было избыточных прав доступа, но и не было препятствий в доступе к действительно необходимым объектам. При этом предоставление прав доступа пользователю к требуемому объекту в рамках дискреционного доступа может быть организовано по различным схемам – через различные цепочки последовательно инициируемых субъектов, через различное сочетание прав доступа по прямым назначениям и прав доступа к объекту, иерархически наследуемых от объектов-контейнеров, в которые входит объект.

Отсюда следует, что задача проектирования системы разграничения доступа (формирование исходного графа доступов Γ_0) имеет не единственное решение, а множество решений. С точки зрения **расширенной модели TAKE-GRANT** каждое такое решение характеризуется своими каналами возможных неявных информационных потоков, выражающиеся, в том числе, и определенными количественными показателями, что может быть использовано в качестве основы критерия для оптимизации системы разграничения доступа.

2.2. Модели безопасности на основе мандатной политики

2.2.1. Общая характеристика политики мандатного доступа

Исходным толчком к разработке мандатной политики, вероятно, послужили проблемы с контролем распространения прав доступа, и, в особенности, проблема «троянских» программ в системах с дискреционным доступом. Исследователи и критики дискреционной политики, понимая, что основная проблема дискреционных моделей заключается в отсутствии контроля за информационными потоками, проанализировали, каким образом подобные проблемы решаются в секретном делопроизводстве.

Было отмечено следующее.

1. Разграничение доступа и порядок работы с конфиденциальными «бумажными» документами организуются на основе парадигмы градации доверия определенным группам работников в отношении государственных секретов определенной степени важности. С этой целью вводится система уровней безопасности, или иначе уровней секретности. Работники с самым высоким уровнем безопасности (уровнем доверия), могут работать с документами самой высокой степени секретности. На более низком уровне доверия, т. е. на более низком уровне безопасности, вводятся ограничения в отношении работы с документами более высокого уровня секретности и т. д. Соответственно, все работники получают т. н. допуск к работе с секретными документами определенного уровня, а документы снабжаются специальной меткой, отражающий требования к уровню безопасности при работе с ними, – т. н. гриф секретности.

2. Критерием безопасности является невозможность получения информации из документов определенного уровня безопасности работником, чей уровень безопасности, т. е. уровень доверия, ниже, чем уровень безопасности соответствующих документов.

Данный критерий безопасности фактически означает запрет определенных информационных потоков, которые трактуются как опасные и недопустимые.

Кроме того, были проанализированы правила и система назначений, изменений, лишений и т. д. допусков сотрудников к работе с секретными документами, правила создания, уничтожения документов, присвоения или изменения грифов их секретности, в том числе и рассекречивания, а также другие особенности работы с секретными документами. В частности, было отмечено, что правила получения доступа к документам различаются в зависимости от характера работы с ними – изучение (чтение) или изменение (создание, уничтожение, внесение дополнений, редактирование, т. е. запись в них). На этой основе было «выявлено» два основных правила, гарантирующих безопасность:

Правило 2.2.1. (no read up (**NRU**) – нет чтения вверх). Работник не имеет права знакомиться с документом (читать), гриф секретности (уровень безопасности) которого выше его степени допуска (уровня безопасности).

Правило 2.2.2. (no write down (**NWD**) – нет записи вниз). Работник не имеет права вносить информацию (писать) своего уровня безопасности в документ с более низким уровнем безопасности (с более низким грифом секретности).

Первое правило является естественным и очевидным способом обеспечения безопасности при осуществлении информационных потоков из документов к работникам и иначе может быть сформулировано так: – работнику нельзя получать информацию, уровень секретности которой выше его уровня доверия. Второе правило обеспечивает безопасность при осуществлении информационных потоков от работника к документу и иначе может быть сформулировано так: – работнику нельзя передавать информацию своего уровня секретности в тех случаях, когда в результате передачи с ней

могут ознакомиться работники с более низким уровнем безопасности.

Формализация данных механизмов разграничения доступа в секретном делопроизводстве применительно к субъектно-объектной модели КС показала необходимость решения ряда следующих задач:

• разработка процедур формализации правила **NRU**, и в особенности правила **NWD**;

• построение формального математического объекта и процедур, адекватно отражающих систему уровней безопасности (систему допусков и грифов секретности).

Нетрудно увидеть, что при представлении работников, работающих с секретными документами, субъектами доступа, а секретных документов в качестве объектов доступа КС, буквальное следование правилу **NWD** приводит к автоматическому включению в механизмы обеспечения безопасности субъективного фактора в лице субъекта-пользователя, который при внесении информации в объекты-документы с более низким грифом секретности должен субъективно оценить соответствие вносимой ин- формации уровню безопасности документа. Задача исключения данного субъективного фактора может решаться различными способами, самым простым из которых является полный запрет изменения субъектами (доступ **write**) объектов с уровнем безопасности, более низким, чем уровень безопасности соответствующих субъектов.

При этом, однако, помимо существенного снижения функциональности КС, логика такого запрета, автоматически приводит к «не запрету» (т. е. к разрешению) возможностей изменения объектов- документов с более высоким уровнем безопасности, чем уровень безопасности соответствующих субъектов-пользователей. Действительно, внесение информации более низкого уровня секретности в объекты с более высоким уровнем секретности не может привести к нарушению безопасности системы в смысле рассмотренного выше критерия безопасности.

В качестве основы для решения второй задачи при создании моделей мандатного доступа был использован аппарат математических решеток. Введем следующие определения.

Определение 2.2.1. Решеткой уровней безопасности $\mathbf{\Lambda_L}$ называется формальная алгебра $\mathbf{\Lambda_L}$ (**L**, ≤, •, ⊗),

где **L** – базовое множество уровней безопасности;

≤ – оператор, который определяет частичное нестрогое отношение порядка для элементов множества **L**, обладающее свойствами антисимметричности, транзитивности и рефлективности:

$\forall\, l \in \mathbf{L}$: $l \le l$ (рефлективность),

$\forall\, l_1, l_2 \in \boldsymbol{L}$: $(l_1 \le l_2 \wedge l_2 \le l_1) \Rightarrow l_1 = l_2$

(антисимметричность);

$\forall\, l_1, l_2, l_3 \in \boldsymbol{L}$: $(l_1 \le l_2 \wedge l_2 \le l_3) \Rightarrow l_1 \le l_3$ (транзитивность);

• – оператор, задающий для любой пары l_1, l_2 элементов множества **L** единственный элемент наименьшей верхней границы:

$$l_1 \bullet l_2 = l \Leftrightarrow l_1, l_2 \le l \wedge \forall\, l' \in \boldsymbol{L}: (l' \le l) \Rightarrow (l' \le l_1 \vee l' \le l_2).$$

⊗ – оператор, задающий для любой пары l_1, l_2 элементов множества L единственный элемент наибольшей нижней границы:

$$l_1 \otimes l_2 = l \Leftrightarrow l \le l_1, l_2 \wedge \forall\, l' \in \boldsymbol{L}: (l' \le l_1 \wedge l' \le l_2) \Rightarrow (l' \le l).$$

Определение 2.2.2. Функцией уровня безопасности $\mathbf{F_L}$ **:X→L** называется однозначное отображение множества сущностей КС

X = S ∪ O во множество уровней безопасности **L** решетки $\mathbf{\Lambda_L}$.

Обратное отображение $\mathbf{F_L^{-1}}$**: L → X** задает разделение всех сущностей КС на классы безопасности $\boldsymbol{X_i}$ такие, что:

$\boldsymbol{X_1 \cup X_2 \cup \ldots \cup X_N = X}$, где N-мощность базового множества уровней безопасности **L**);

$$\boldsymbol{X_i \cap X_j \equiv \varnothing}, \text{ где } i \ne j;$$

$$\forall\, x' \in X_i \Rightarrow \mathfrak{F}_L(x') = l_i,\ l_i \in \mathbf{L}.$$

Покажем, что введенные решетка и функция уровней безопасности адекватно отражают парадигму градуированного доверия и критерий безопасности систем на ее основе.

1. Предположим, что информация может передаваться от сущностей класса X_i к сущностям класса X_j и наоборот, т. е. от сущностей класса X_j к сущностям класса X_i. Тогда для выполнения критерия безопасности сущности классов X_i и X_j должны образовывать один общий класс X_{ij}. Для того чтобы не создавать избыточных классов, необходимо, чтобы отношение, задаваемое оператором доминирования $\leq$, было антисимметричным.

2. Предположим, что информация может передаваться от сущностей класса X_i к сущностям класса X_j, и, кроме того, от сущностей класса X_j к сущностям класса X_k. Если каждая такая передача безопасна в отдельности, то, очевидно, безопасна и передача информации от сущностей класса X_i к сущностям класса X_k. Таким образом, отношение, задаваемое оператором $\leq$, должно быть транзитивным.

3. Внутри класса сущности имеют одинаковый уровень безопасности. Следовательно, передача информации между сущностями одного класса безопасна. Отсюда следует сравнимость по оператору $\leq$ сущностей одного класса между собой и самих с собой, т. е. рефлективность отношения $\leq$.

4. Предположим, что имеется два различных класса сущностей X_i и X_j. Тогда, из соображений безопасности очевидно, что существует толь- ко один класс X', потоки от сущностей которого безопасны по отношению к сущностям класса X_i или класса X_j , совпадающий с классом X_i или с классом X_j , и не имеется никакого другого класса X'', менее безопасного чем X', и с такими же возможностями по потокам к сущностям классов X_i и X_jЭто означает, что X' должен быть

наименьшей верхней границей по уровням безопасности классов X_i и X_j .

5. Аналогично по условиям предыдущего пункта должен существовать ближайший снизу к классам X_i и X_j класс X', такой, что потоки от сущностей классов X_i и X_j к сущностям класса X' безопасны, и совпадающий с классом X_i или с классом X_j , при этом не имеется никакого другого класса X" , более безопасного, чем X' , и с такими же возможностями по потокам от сущностей классов X_i и X_j. Это означает, что X' должен быть наибольшей нижней границей по уровням безопасности классов X_i и X_j.

Таким образом, аппарат решетки и функция уровней безопасности действительно адекватно отражают сущность принципов и отношений политики мандатного разграничения доступом, на базе которых строятся конкретные модели, специфицирующие, в том числе, формализацию правил **NRU** и **NWD**, а также другие особенности мандатного доступа.

В заключение общей характеристики политики мандатного доступа отметим, что в ней разграничение доступа осуществляется до уровня классов безопасности сущностей системы. Иначе говоря, любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил **NRU** и **NWD**). Нетрудно видеть, что мандатный подход к разграничению доступа, основываясь только лишь на идеологии градуированного доверия, без учета специфики других характеристик субъектов и объектов, приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующих классов безопасности, что противоречит самому понятию разграничения доступа. Для устранения данного недостатка мандатный принцип разграничения доступа дополняется дискреционным внутри соответствующих классов безопасности. В теоретических моделях для этого вводят матрицу доступа, разграничивающую разрешенный по

мандатному принципу доступ к объектам одного уровня безопасности.

2.2.2. Модель Белла-ЛаПадулы и ее расширения

Первой формальной моделью мандатного доступа является модель, разработанная еще в 1972–1975 г.г. американскими специалистами – сотрудниками MITRE Corporation Дэвидом Беллом и Леонардом ЛаПадулой (D.Elliott **Bell**, Leonard **J.LaPadula**), названная по их имени и сыгравшая огромную методологическую роль в развитии теории компьютерной безопасности.

Основные положения модели Белла-ЛаПадулы сводятся к следующему.

1. Модель системы $\Sigma(v_0, Q, F_T)$ представляется совокупностью:

- множества объектов **O** доступа;
- множества субъектов **S** доступа;
- множества прав доступа **R** (в т. н. «классической» модели Белла- ЛаПадулы) всего два элемента – **read** и **write**);
- матрицы доступа **A[s,o]**;
- решетки Λ_L уровней безопасности L субъектов и объектов системы;
- функции F_L: **S** ∪ **O** → **L**, отображающей элементы множеств **S** и **O** на множество **L**;
- множества состояний системы **V**, которое определяется множеством упорядоченных пар (F_L, **A**);
- начального состояния $v_0 \in$ **V**;
- набора запросов **Q** субъектов на доступ (осуществление операций) к объектам, выполнение которых переводит систему в новое состояние;
- функции переходов $F_T : (V \times Q) \to V^*$, которая переводит систему из одного состояния **V** в другое **V*** при выполнении запросов из **Q**.

Состояния системы разделяются на опасные и безопасные. Для анализа и формулировки условий, обеспечивающих безопасность состояний системы, вводятся следующие определения:

Определение 2.2.3. Состояние называется безопасным по чтению (или просто безопасным) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта:

$$\forall s \in S, \forall o \in O, read \in A[s, o] \rightarrow \mathcal{F}_L(s) \geq \mathcal{F}_L(o).$$

Определение 2.2.4. Состояние называется безопасным по записи (или *-безопасным) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта:

$$\forall s \in S, \forall o \in O, write \in A[s, o] \rightarrow \mathcal{F}_L(o) \geq \mathcal{F}_L(s).$$

Определение 2.2.5. Состояние системы безопасно тогда и только тогда, когда оно безопасно и по чтению, и по записи.

На основе введенных понятий, которые, как нетрудно видеть, выражают правила **NRU** и **NWD** политики мандатного доступа, авторы модели сформулировали следующий критерий безопасности.

Определение 2.2.6. (Критерий безопасности в модели Белла-ЛаПадулы). Система $\Sigma(v_0, Q, \mathcal{F}_T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из **Q**, безопасны.

На основе данного критерия Белл и ЛаПадула доказали теорему, получившую название «основной теоремы безопасности» (**ОТБ**).

Теорема 2.2.1.(Basic Security Theorem). Система $\Sigma(v_0, Q, F_T)$безопасна тогда и только тогда, когда:

1. Состояние v_0 безопасно, и

2. Функция переходов F_T такова, что для любого состояния v, достижимого из v_0 при выполнении конечной последовательности запросов из множества Q таких, что при F_T **(v,q)=v***, где **v=(F_L,A)** и **v*=(F_L*,A*)**, переходы системы из состояния в состояние подчиняются следующим ограничениям для s ∈ **S** и для o ∈ **O**

- если **read ∈ A*[s, o]** и **read ∈A[s, o],** то F_L***(s) ≥** F_L***(o);**
- если **read ∈ A[s, o]** и F_L***(s) <** F_L***(o),** то **read ∉ A*[s, o];**
- если **write ∈ A*[s, o]** и **write ∉A[s, o],** то F_L***(s) ≥** F_L ***(o);**
- если **write ∈ A[s, o]** и F_L***(s) <** F_L***(o),** то **write ∉A*[s, o]**

.

Модель Белла-ЛаПадулы сыграла огромную роль в развитии теории компьютерной безопасности, и ее положения были введены в качестве обязательных требований к системам, обрабатывающим информацию, содержащую государственную тайну, в стандартах защищенных КС, в частности, в известной «Оранжевой книге» (1983 г.). Одной из сильных сторон модели Белла-ЛаПадулы является автоматическое решение проблемы «троянских» программ. Процесс переноса информации с помощью «троянской» программы из объекта, доступ к которому субъекту не разрешен по матрице доступа, регламентируется, как и любые другие потоки принципами **NRU** и **NWD**. Таким образом, если такой перенос информации и произойдет, то он будет укладываться в ограничения определений 2.2.3 и 2.2.4, и, следовательно, с точки зрения критерия безопасности по определению2.2.6 система останется в безопасном состоянии.

2.2.3. Основные расширения модели Белла-ЛаПадулы

При практической реализации положений модели Белла-ЛаПадулы в реальных КС возник ряд трудностей, послуживших основанием для многочисленных работ по ее критическому анализу. Основные из этих трудностей связаны с проблемами переходных процессов, изменяющих доверительные характеристики (уровни безопасности) субъектов и объектов доступа, а также с невозможностью ограничиться в реальных КС процессами, сопровождающимися только лишь однонаправленными информационными потоками. В частности, один из наиболее известных исследователей модели Белла-ЛаПадулы, МакЛин привел концептуальное описание **Z**- системы, удовлетворяющей условиям **ОТБ**, но, вместе с тем, обеспечивающей возможность получения доступа любым субъектом к любому объекту по любому методу (**read** и **write**). В **Z**-системе субъекты и объекты в промежутках переходов системы из одного состояния в другое имеют возможности изменять свой уровень безопасности, при этом ни одно из ограничений **ОТБ** не нарушается. Тем не менее, последовательно снижая классификацию (уровень) объекта до своего уровня, или вовсе его деклассифицируя, субъект может получить доступ по чтению к нужному объекту. Также, последовательно понижая свой уровень безопасности, субъект может получить доступ к нужному объекту по записи.

Причина проблемы **Z**-системы, как указал МакЛин, в том, что модель Белла-ЛаПадулы никаким образом не специфицирует и не регламентирует процессы назначения и изменения уровня безопасности сущностей системы, т. е. является чрезмерно абстрактной по отношению к реальным процессам в КС.

Проведя обстоятельные и глубокие исследования классической модели Белла-ЛаПадулы, МакЛин построил несколько расширений модели Белла-ЛаПадуллы, преодолевающих некоторые недостатки или приближающих к

«реальности» исходную каноническую модель. Первое из этих расширений связано с исследованием условий и ограничений, накладываемых на функцию перехода (модель с **безопасной функцией перехода**).

Для рассмотрения условий безопасности функции перехода МакЛин разделил общую функцию уровней безопасности $\mathcal{F}_L$: **S ∪ O→ L** на функцию уровней безопасности субъектов $\mathcal{F}_{L_S}$: **S → L** и функцию уровней безопасности объектов $\mathcal{F}_{L_O}$: **O → L.**

В модели с безопасной функцией переходов на этой основе вводятся следующие определения.

Определение 2.2.7. Функция перехода $\mathcal{F}_T$: **(V x Q) → V** является безопасной по чтению, если для любого перехода $\mathcal{F}_T$ **(v,q)=v*** выполняются следующие три условия:

- если **read ∈ A*[s,o]** и **read ∉A[s,o],** то $\mathcal{F}_{L_S}$ **(s)≥** $\mathcal{F}_{L_O}$ **(o)** и $\mathcal{F}_L = \mathcal{F}_L$* ;

- если $\mathcal{F}_{L_S} \neq \mathcal{F}_{L_S}$*, то **A=A***, $\mathcal{F}_{L_O}$= $\mathcal{F}_{L_O}$*, для ∀**s** и **o**, у которых $\mathcal{F}_{L_S}$ ***(s)** < $\mathcal{F}_{L_O}$***(o)**, **read ∉ A[s, o]**;

- если $\mathcal{F}_{L_O} \neq \mathcal{F}_{L_O}$*, то **A=A***, $\mathcal{F}_{L_S} = \mathcal{F}_{L_S}$ *, для ∀**s** и **o**, у которых $\mathcal{F}_{L_S}$***(s)** < $\mathcal{F}_{L_O}$***(o), read ∉ A[s, o]**.

Определение 2.2.8. Функция перехода $\mathcal{F}_T$: **(V x Q) → V** является безопасной по записи, если для любого перехода $\mathcal{F}_T$ **(v,q)=v*** выполняются следующие три условия:

- если **write ∈ A*[s, o]** и **write ∉ A[s, o]**, то $\mathcal{F}_{L_S}$ **(s)≥** $\mathcal{F}_{L_O}$ **(o)** и $\mathcal{F}_L = \mathcal{F}_L$* ;

- если $\mathcal{F}_{L_S} \neq \mathcal{F}_{L_S}$ *, то **A=A***, $\mathcal{F}_{L_O}$= $\mathcal{F}_{L_O}$*, для ∀**s** и **o**, у которых $\mathcal{F}_{L_S}$ ***(s)** > $\mathcal{F}_{L_O}$***(o), write ∉ A[s, o**];

- если $\mathcal{F}_{L_O} \neq \mathcal{F}_{L_O}$*, то **A = A*,** $\mathcal{F}_{L_S} = \mathcal{F}_{L_S}$ ***,** для ∀**s** и **o**, у которых $\mathcal{F}_{L_S}$***(s)** > $\mathcal{F}_{L_O}$***(o), write ∉ A[s, o]**.

Определение 2.2.9 (Критерий безопасности МакЛина). Функция перехода f_T: **(V x Q) → V** является безопасной тогда и только тогда, когда она безопасна и по чтению, и по записи.

Смысл ограничений на безопасность функции перехода в определениях 2.2.8 и 2.2.9 в неформальном выражении заключается в том, что в процессе перехода может меняться, во-первых, только лишь один из компонентов состояния системы безопасности (или отношение доступа определенного субъекта к определенному объекту, т. е. ячейка матрицы доступа, или решетка уровней безопасности субъектов, или решетка уровней безопасности объектов), а, во-вторых, при условии того, что правила **NRU** и **NWD** соблюдаются как в предыдущем, так и в новом состоянии.

Основываясь на введенных определениях, МакЛин сформулировал и доказал следующую теорему.

Теорема 2.2.2. (Теорема безопасности МакЛина). Система $\Sigma(v_0, Q, f_T)$ безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние v_0 безопасно, а ее функция перехода удовлетворяет критерию безопасности МакЛина.

Условия безопасности переходов МакЛина снимают проблему **Z**- системы, но, тем не менее, не решают всех проблем практической реализации КС на основе модели Белла-ЛаПадулы. В частности, введенные условия по определениям 2.2.7 и 2.2.8 накладывают ограничения, но не специфицируют сам процесс изменения уровней безопасности сущностей системы. Иначе говоря, вопросы о том, кто, при каких условиях имеет право изменять уровни безопасности сущностей системы (т. е. инициировать соответствующие переходы), по-прежнему остаются неопределенными.

МакЛин для решения данной проблемы расширил модель Белла-ЛаПадулы введением **уполномоченных субъектов.**

Определение 2.2.10. Подмножество субъектов **P(S)**, которым разрешается инициировать переходы системы, изменяющие уровни безопасности субъектов или объектов, называется уполномоченными (доверенными) субъектами.

На этой основе в модели вводится дополнительная функция управления уровнями безопасности.

Определение 2.2.11. Функцией управления уровнями безопасности f_C: **S ∪ O → P(S)** называется отображение множества сущностей КС (субъектов и объектов) на подмножество уполномоченных субъектов.

Заметим, что в общем виде функция f_C задается не однозначным отображением и определяет тем самым в системе с уполномоченными субъектами для каждого объекта или субъекта одного, или нескольких субъектов, которым разрешено изменять уровни безопасности соответствующих сущностей.

Реализация системы с уполномоченными субъектами требует изменения также и функции перехода системы, а именно, ее авторизации.

Определение 2.2.12. Функция перехода f_T^A: **(S x V x Q) → V** в системе с уполномоченными субъектами $\Sigma(v_0, Q, f_T^A)$ называется авторизован- ной тогда и только тогда, когда для каждого перехода t^A**(s, v, q) = v***, при котором **v = (**f_T**, A)** и **v* = (**f_T***, A*)**, выполняется следующее условие: ∀ **x ∈ S ∪ O**: если f_L*(**x**) ≠ f_L (**x**), то **x ∈ P(S)**.

Аппарат уполномоченных субъектов на основе определений 2.2.10, 2.2.11 и 2.2.12 разрешает неопределенность процессов изменения уровней безопасности сущностей системы в абстрактной модели Белла-ЛаПадулы и позволяет разработчикам специфицировать и строить реальные КС с мандатным принципом разграничения доступа.

Вместе с тем, введение уполномоченных субъектов не обеспечивает автоматически всех условий и ограничений

безопасности, а только лишь специфицирует процесс изменения уровней безопасности сущностей системы. Следовательно, вопросы безопасности функционирования системы с уполномоченными субъектами должны в достаточном отношении рассматриваться с точки зрения дополнительных условий, определяемых **ОТБ** и теоремой МакЛина (по безопасной функции перехода).

Более того, внимательный анализ идеологии уполномоченных субъектов показывает наличие внесения в процессы безопасности субъективного фактора. Доверенные субъекты, изменяя уровни безопасности субъектов и объектов системы, должны действовать корректно, к примеру, снижать гриф секретности объекта, когда из него удалена вся информация более высокого уровня и т. П

Очевидно, как некая альтернатива уполномоченным субъектам, избавляющая процессы безопасности от субъективного фактора, была предложена мандатная **модель Low-Watermark (LWM).**

Неформальное выражение существа модели **LWM** сводится к следующему. Если по определенным соображениям субъектам нельзя отказывать в доступе **write** к любым объектам системы, то для исключения опасных информационных потоков «сверху вниз», т. е. от сущностей с высоким уровнем безопасности к сущностям с более низким уровнем безопасности, необходимо дополнить определенными правилами операцию **write** и ввести дополнительную операцию **reset.**

Если субъекту требуется внести информацию в объект с более низким, чем у субъекта, уровнем безопасности (что запрещено правилом **NWD**), то субъект может подать команду **reset**, в результате которой уровень безопасности объекта автоматически повышается до максимального уровня безопасности в системе. В результате операции **reset** объект согласно правилу, **NWD** становится доступным по записи (в том числе и для всех других субъектов системы). При этом, однако, опасности перетекания информации «сверху вниз» не

создается, так как по чтению система как прежде, так и в дальнейшем руководствуется безопасным правилом **NRU**.

Нетрудно увидеть, что данный порядок порождает тенденцию деградации (огрубления) системы разграничения доступа, при которой все объекты через какое-то время могут получить высшие грифы секретности и, соответственно, стать недоступными по чтению для всех субъектов, не обладающих высшим уровнем доверия. Поэтому в модели **LWM** операция **write** дополняется следующим условием. Если в результате операции **write** в объект реально вносится информация и уровень безопасности объекта строго выше уровня безопасности субъекта, то перед внесением в объект информации вся прежняя информация из него удаляется (стирается), а по окончании операции записи уровень безопасности объекта автоматически понижается до уровня безопасности субъекта.

В модели **LWM** доказывается, что введение операции **reset** и видоизмененной операции **write** оставляет систему безопасной в смысле критерия безопасности Белла-ЛаПадулы.

От себя заметим, что более логичным, но в определенном смысле зеркальным по отношению к модели **LWM**, мог бы быть подход, при котором субъектам разрешается производить запись в объекты с более низким уровнем безопасности при условии того, что при завершении операции уровень безопасности объекта автоматически повышается до уровня безопасности субъекта. При этом возможность опасных потоков «сверху вниз» также, как и в модели **LWM** нейтрализуется.

Еще одним расширением модели Белла-ЛаПадулы, имеющим важное прикладное значение, является введение методологии и техники **совместного (группового) доступа.**

Как уже отмечалось, политика и, соответственно, модели мандатного доступа основываются на принципах, заимствованных из правил и системы секретного делопроизводства, принятых во многих странах, в частности в США. Одним из таких правил, является то, что некоторые

наиболее критичные с точки зрения безопасности процессы, например, изменение уровня конфиденциальности документов, осуществляются путем совместных действий (одновременных или последовательных) нескольких работников – исполнителя (владельца) документа и руководителя (администратора).

Подобные приемы усиления безопасности применяются и в других сферах, например, в бухгалтерии, где критичные операции приема/выдачи финансовых средств осуществляются совместными действиями кассира и контроллера, каждый из которых подписывает или заверяет соответствующий платежный документ. Еще одним из подобных правил является порядок доступа к индивидуальным ячейкам-хранилищам клиентов банков, когда для их открытия требуется одновременно два ключа – один от клиента, другой от служащего (администратора) банка.

Для реализации технологии совместного доступа в мандатной модели добавляется функция группового доступа.

Определение 2.2.13. Функцией группового доступа F_G: **S** → **P(S)** \ ∅ называется отображение множества субъектов КС **S** на множество непустых подмножеств субъектов S_G = **P(S)** \ ∅, каждое из которых образует групповой субъект доступа $s_G \in S_G$.

На этой основе в матрице доступа **A[s,o]** системы добавляются строки, соответствующие субъектам группового доступа.

Помимо дополнения матрицы доступа системы групповыми субъектами, требуется также разработка механизмов реализации для них правил мандатного доступа, т. е. правил NRU и NWD, имея ввиду то, что в состав подмножества субъектов, образующих субъект группового доступа, могут входить субъекты с различным уровнем безопасности. С этой целью вводятся дополнительные функции уровней безопасности субъектов группового доступа.

Определение 2.2.14. Функцией уровня безопасности F_L^L : **SG→ L** называется однозначное отображение множества субъектов группового множества S_G во множество уровней безопасности **L** решетки **Λ** такое, что $F_L^L(s_G)$ является наибольшей нижней границей уровней безопасностей для множества субъектов **s**, входящих в s_G .

Определение 2.2.15. Функцией уровня безопасности F_L^H : **SG→ L** называется однозначное отображение множества субъектов группового множества S_G во множество уровней безопасности **L** решетки **Λ** такое, что $F_L^H(s_G)$ является наименьшей верхней границей уровней безопасностей для множества субъектов s, входящих в s_G.

Введение функций F_L^L и F_L^H дает возможность переопределить критерий безопасности (определения 2.2.4, 2.2.5 и 2.2.6) исходной модели мандатного доступа Белла-ЛаПадулы.

Определение 2.2.16. Состояние системы называется безопасным по чтению тогда и только тогда, когда для каждого индивидуального или группового субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности, задаваемый функцией F_L для индивидуального субъекта или функцией F_L^L для группового субъекта, доминирует над уровнем безопасности объекта.

Определение 2.2.17. Состояние системы называется безопасным по записи тогда и только тогда, когда для каждого индивидуального или группового субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности объекта доминирует над уровнем безопасности субъекта, задаваемого функцией F_L для индивидуального субъекта или функцией F_L^H для группового субъекта.

Иными словами, доступ по чтению для групповых субъектов безопасен тогда, когда самый низший уровень безопасности из множества индивидуальных субъектов, образующих групповой субъект, выше или равен уровню безопасности объекта чтения. Доступ по записи для групповых объектов безопасен тогда, когда самый высокий уровень безопасности из всех индивидуальных субъектов, входящих в групповой субъект, ниже или равен уровню безопасности объекта записи.

Остальные условия безопасного функционирования системы с субъектами группового доступа задаются условиями соответствующих теорем (**ОТБ** или теоремы МакЛина).

Таким образом, расширения модели Белла-ЛаПадулы обеспечивают устранение многих недостатков исходной модели, и, кроме того, могут комбинироваться для обеспечения более реализуемых на практике спецификаций политики мандатного доступа в реальных КС.

Тем не менее, расширения модели Белла-ЛаПадулы не снимают всех недостатков мандатного доступа. В частности, как уже указывалось, мандатный доступ снимает проблему «троянских программ», но только с точки зрения опасных потоков «сверху вниз». Однако в пределах одного класса безопасности, вопросы доступа решаются, как и в дискреционных моделях, на основе матрицы доступа, и, следовательно, для полного устранения проблемы «троянских программ» и в системах мандатного доступа требуется более тщательный и детализированный контроль информационных потоков, в том числе механизмов ИПС.

2.3. Модели безопасности на основе тематической политики

2.3.1. Общая характеристика тематического разграничения доступа

Как уже не раз отмечалось многие механизмы и принципы разграничения доступа к информации «подсмотрены» во внекомпьютерной сфере, что обеспечило формирование двух базовых политик безопасности – дискреционного и мандатного доступа. Вместе с тем, данные политики безопасности отражают не все организационно-технологические схемы защиты конфиденциальной информации, исторически наработанные и апробированные в «бумажных» сферах.

Важным аспектом, присутствующим в практике разграничения доступа к «бумажным» ресурсам является тематическая «окрашенность» информационных ресурсов предприятий, учреждений по организационно-технологическим процессам и профилям деятельности. Организация доступа сотрудников к информационным ресурсам организации (в библиотеках, архивах, документальных хранилищах) осуществляется на основе тематических классификаторов. Все документы информационного хранилища тематически индексируются, т. е. соотносятся с теми или иными тематическими рубриками классификатора. Сотрудники предприятия согласно своим функциональным обязанностям или по другим основаниям получают права работы с документами определенной тематики. Данный подход, в сочетании с избирательным и мандатным доступом, обеспечивает более адекватную и гибкую настройку системы разграничения доступа на конкретные функционально-технологические процессы, предоставляет дополнительные средства контроля и управления доступом.

Помимо уже указанной MLS-решетки, попытки отразить тематический аспект в организации разграничения доступа, имелись еще в ранних работах по моделям дискреционного

доступа, в частности, в одной из первых дискреционных моделей АДЕПТ-50, в модели на основе типизованной матрицы доступа, в расширениях базовой модели безопасности ОС UNIX – модели **DTE**. Вместе с тем, использование тематических категорий субъектов и объектов доступа в данных моделях являлось второстепенным фактором, служащим для уточнения или корректировки некоторых аспектов базовой политики безопасности. Кроме того, назначение субъектам и объектам доступа единичных категорий из простого неупорядоченного списка тематик обеспечивает лишь наиболее простой и грубый способ тематического разграничения доступа к информации.

В общем плане принцип тематической политики безопасности можно пояснить схемой, приведенной на рис. 2.13.

Рис. 2.13. Общий принцип тематической политики безопасности

Анализ библиотечных и других автоматизированных систем документального поиска, основанных на тематическом индексировании содержания документов (текстов), показывает, что определяющее значение в таких системах имеет тематико-классификационная схема, в большинстве случаев именуемая

тематическим рубрикатором. Применяются три основных способа тематической классификации:

• перечислительная классификация (дескрипторный подход);

• систематизированная классификация (иерархический подход);

• аналитико-синтетическая классификация (фасетный подход).

При дескрипторном подходе классификационная схема представляет неупорядоченный перечень тематик (рубрик, предметов, ключевых слов и т. д.), произвольной совокупностью которых можно отразить содержание (тематику) конкретного документа – см. рис. 2.14.

Сотрудники предприятия получают права работы с документами определенного набора тематических рубрик, т.е. фактически так же, как и документальные ресурсы тематически классифицируются.

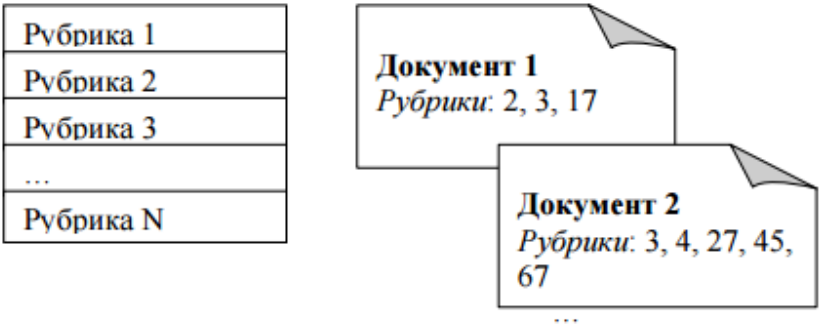

Рис. 2.14. Дескрипторная классификация

При иерархическом подходе тематико-классификационная схема представляет корневую древовидную структуру, основанную на таксономическом принципе («род-вид»). Тематика документа определяется тематическими узлами классификатора с автоматическим распространением на объект классификации всех

соответствующих подчиненных тематических узлов – см. рис. 2.15. Сотрудникам предприятия предоставляется право работы с документами, тематика которых соответствует одному или нескольким узлам классификатора с автоматическим распространением прав работы на документы с тематикой соответствующих подчиненных узлов.

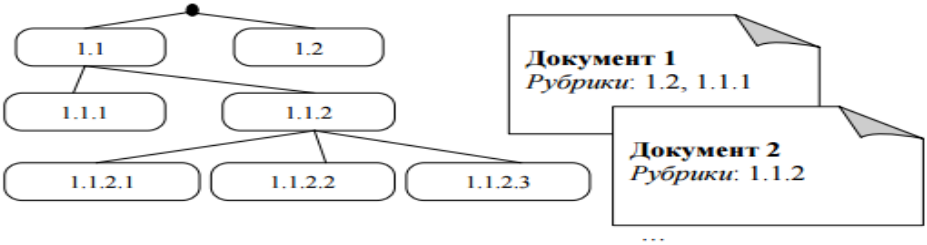

Рис. 2.15. Иерархическая классификация

Основу фасетной классификации составляет определенное количество тематических блоков-фасет, отражающих логику соответствующей предметной сферы (например, «материал»-«конструкция»-«нагрузки» или «время»-«место»-«состав»-«действие» и т. д.). Каждый фасет, в свою очередь, представляет классификационную подсистему тематик (рубрик) иерархического типа. Тематика конкретного информационного объекта строится на основе сочетания тематических узлов фасетных рубрик – см. рис. 2.16. Права доступа сотрудников к документам определяются также сочетанием определенных рубрик по фасетам классификатора.

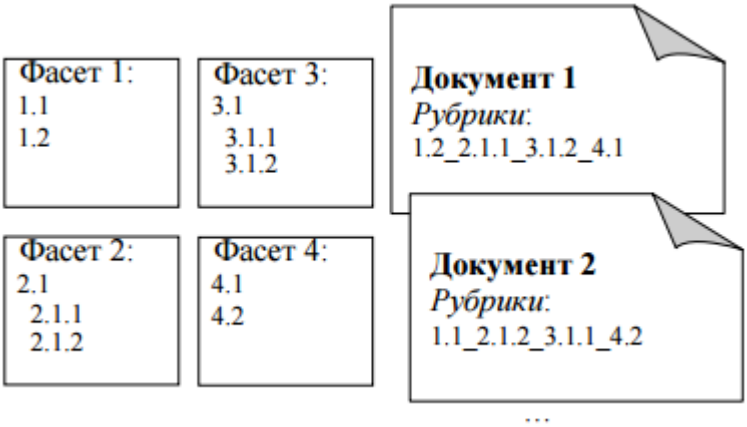

Рис. 2.16. Фасетная классификация

Общим правилом (критерием) предоставления доступа пользователям к ресурсам (объектам) по всем способам классификации является следующее:

Определение 2.3.1 (Общее правило тематического доступа). Документ доступен сотруднику, если он не содержит рубрик, запрещенных (не разрешенных) для данного сотрудника.

В документальных хранилищах, библиотеках и архивах ввиду их очевидного предназначения под доступом понимается, прежде всего, чтение документов. Иначе говоря, в данных системах присутствует перенос информации (информационные потоки) только из документов к сотрудникам.

В системах, где документы не только изучаются, используются, но и создаются, корректируются (например, системы делопроизводства и документооборота), возможны как потоки из документов к сотрудникам, так от сотрудников в документы. Однако, совершенно ясно, что в «бумажном контуре» при создании и, в особенности, при изменении документов вносить или изменять информацию в документ, не «видя» все остальное содержимое документа невозможно.

Поэтому, в отличие от правила **NWD** мандатного доступа, кстати сказать, огрубленного и идеалистически абстрактного для реализации в «бумажном контуре», в системах делопроизводства в большинстве случаев используются следующие правила:

• тематика создаваемого (редактируемого) документа назначается (уточняется) исполнителем документа (автором, ответственным и т. д.) в пределах тематики данного исполнителя;

• создание или изменение документов может происходить на основе объединения (слияния) в один общий документ совокупности других документов, при этом тематика общего документа формируется как объединенная тематика совокупности вошедших в него документов, а процедуру объединения (слияния) осуществляет сотрудник, допущенной ко всей объединенной тематике.

Отмеченные правила преследуют цель обеспечения конфиденциальности (безопасности) информации в системе, что можно сформулировать следующим общим критерием безопасности тематического разграничения доступа.

Определение 2.3.2 (Критерий безопасности тематического доступа). Система безопасна, если пользователи ни при каких обстоятельствах не могут получить доступ к информации «не своей» тематики.

Система и порядок тематического разграничения доступа регламентируются нормативными документами предприятий, организаций, ведомств, и совершенно очевидно, что, автоматизируя документальные информационные системы, подобные регламентации необходимо воспроизводить в виде формализованных процедур, схем представления и манипулирования с информацией в КС, т. е. в виде моделей тематического разграничения доступа.

2.3.2. Тематические решетки

Как и в моделях мандатного доступа, контроль безопасности информационных потоков при тематическом доступе базируется на использовании аппарата решеточно упорядоченных множеств.

Результаты дескрипторной тематической классификации сущностей системы (тематики $\mathcal{F}_{Д}[x_i]$) образуют тематическую решетку, являющуюся решеткой подмножеств $\Lambda_{Д}(\mathcal{P}_{Д}, \subseteq, \cup, \cap)$множества $T_{Д}$ ($\mathcal{P}_{Д}$ – множество подмножеств множества $T_{Д}$).

Частичный порядок на множестве $\mathcal{P}_{Д}$ задается отношением теоретико-множественного включения $\subseteq$, определяющего доминирование тематической классификации сущности x_i над тематической классификацией сущности x_j в том случае, когда $\mathcal{F}_{Д}[x_j] \subseteq \mathcal{F}_{Д}[x_i]$. При этом отношение, задаваемое операцией включения, обладает свойствами рефлексивности, антисимметричности и транзитивности. Наименьшая верхняя и наибольшая нижняя граница для любой пары тематических классификаций сущностей системы $\mathcal{F}_{Д}[x_i]$ и $\mathcal{F}_{Д}[x_j]$ задаются операциями теоретико-множественного объединения $\mathcal{F}_{Д}[x_i] \cup \mathcal{F}_{Д}[x_j]$ и пересечения $\mathcal{F}_{Д}[x_i] \cap \mathcal{F}_{Д}[x_j]$], соответственно.

При иерархической тематической классификации применяются монорубрицированный и мульти-рубрицированный подходы, соответствующие двум различным направлениям в архитектуре и механизмах функционирования информационно-поисковых документальных систем.

Определение 2.3.8. Монорубрицированной иерархической тематической классификацией $\mathcal{F}_{И1}[x]$ называется отображение множества сущностей системы **X= S ∪ O** на множество тематических рубрик иерархического классификатора $T_{И}$ такое, что любой сущности системы **x ∈ X**

соответствует определенная и единственная тематическая рубрика $\tau \in T_и$ совместно со всеми подчиненными узлу τ рубриками.

Таким образом, в системах с монорубрицированным отображением каждому объекту о соответствует определенная и единственная тематическая рубрика τ (узел корневого дерева) с автоматическим включением в характеристику информационного содержания объекта о тематики всех узлов рубрикатора, подчиненных узлу τ. Данный подход, характеризует инфологическую сущность информационно-поисковых каталогов, в которых объекты доступа (документы) технологически размещаются в узлах каталога. При этом структура каталога собственно и выражает тематический рубрикатор.

Определение 2.3.9. Мультирубрицированной иерархической тематической классификацией $F_{и2}[x]$ называется отображение множества сущностей системы $\mathbf{X = S \cup O}$ на множество тематических рубрик иерархического классификатора $T_и$ такое, что любой сущности системы $\mathbf{x \in X}$ соответствует набор тематических рубрик $\{\tau_{x_1}, \tau_{x_2}, \dots\}$, причем рубрики $\tau_{x_1}, \tau_{x_2}, \cdots$ не находятся между собой в подчинении и никакая их совокупность не образует полный набор сыновей какого-либо узла классификатора.

Первое условие в определении мультирубрицированной классификации обусловлено тем, что если сущность КС отображается на определенный узел корневого дерева, то по смыслу иерархически организованного множества $T_и$ данное отображение включает и все подчиненные по дереву соответствующие узлы. Отсюда явно включать в классификацию узлы, находящиеся между собой в иерархическом подчинении, не имеет никакого смысла.

Второе условие обусловлено тем, что если определенная совокупность узлов составляет полный набор узлов, являющихся непосредственными потомками какого-либо узла

дерева, то по таксономическому свойству иерархического рубрикатора это означает, что в данной ситуации вместо подобной совокупности узлов достаточно использовать узел-родитель.

Таким образом в системах с мультирубрицированным отображением каждому объекту о может соответствовать не одна, а некоторая совокупность тематических рубрик $\{\tau_{o1}, \tau_{o2}, \dots\}$, т. е. узлов корневого дерева, при условии того, что данные узлы не находятся в отношении друг друга в иерархическом подчинении и никакая их совокупность не образует полный набор сыновей какого-либо иерархического узла. При этом в характеристику информационного содержания объекта о включается также тематика всех узлов рубрикатора, подчиненных узлам $\tau_{o1}, \tau_{o2}, \dots$. Подобный подход характерен для индексных информационно-поисковых систем, строящихся на основе иерархических рубрикаторов, в частности, для информационно- поисковых систем, основанных на тезаурусах.

Тематические разрешения пользователям в системах и первого и второго вида, иначе говоря, отображения субъектов доступа на множество вершин иерархического рубрикатора, в большинстве случаев производится мультирубрицированным образом.

Тематическая решетка при монорубрицированном отображении на множестве $\boldsymbol{T_и} = \{\tau_1, \tau_2, \dots, \tau_M\}$ корневое дерево иерархического рубрикатора задает отношение частичного порядка $\leq$, обладающее свойствами рефлективности, антисимметричности и транзитивности.

Для построения решетки на множестве $\boldsymbol{T_и}$ помимо отношения частичного порядка необходимо задать операции (механизмы), определяющие для любой пары рубрик (τ_i, τ_j) наименьшую верхнюю и наибольшую нижнюю границы.

Дополняя множество $\boldsymbol{T_и}$ пустой рубрикой (элементом τ_0) и замыкая на него все концевые (листовые) вершины (см. рис. 2.17), получаем решеточно упорядоченное множество, в

котором для любой пары элементов $\{\tau_i, \tau_j\}$ имеется наименьшая верхняя $\sup\{\tau_i, \tau_j\}$ и наибольшая нижняя граница $\inf\{\tau_i, \tau_j\}$.

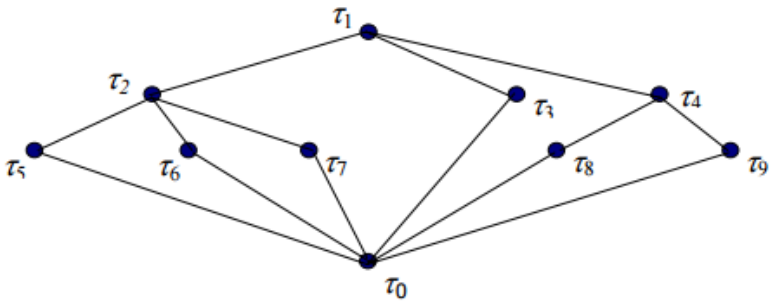

Рис. 2.17. Переход к решеточно упорядоченному множеству путем добавления пустого элемента

Определение 2.3.10. Наименьшей общей верхней границей sup**и** $\{\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}\} = \tau_i$ для набора рубрик $\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}$ будем называть вершину τ_i, являющуюся по корневому дереву иерархического рубрикатора наименьшим общим предком вершин $\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}$.

Определение 2.3.11. Наибольшей общей нижней границей inf**и** $\{\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}\} = \tau_i$ для набора рубрик $\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}$ будем называть вершину τ_i, являющуюся в графе, образованном корневым деревом иерархического рубрикатора с замыканием всех его листовых вершин на пустую вершину, наибольшей общей подчиненной вершиной рубрик $\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}$.

При этом из определения 2.3.11 следует, что если вершины $\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_k}$ попарно сравнимы, т. е. находятся на разных уровнях одной ветви дерева, то наибольшей нижней границей inf**и** является вершина, находящаяся на самом нижнем уровне соответствующего участка данной ветви

дерева, т. к. является ближайшей, подчиненной снизу всем, включая саму себя из набора $\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_k}\}$. При несравнимости (неподчиненности друг другу) хотя бы в одной паре рубрик произвольного набора $\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_k}$ наибольшим общим потомком inf**и** является пустая вершина τ_0, которую можно трактовать как отсутствие в объекте классификации информации, описываемой иерархическим рубрикатором.

В результате на множестве $\boldsymbol{T}_{\text{и}\varnothing} = \boldsymbol{T}_{\text{и}} \cup \tau_0$ имеем решетку $\boldsymbol{\Lambda}_{\text{и}}(\boldsymbol{T}_{\text{и}\varnothing}, \leq, \sup\textbf{и}, \inf\textbf{и})$, основывая на которой монорубрицированную тематическую классификацию сущностей системы можно построить модель тематического разграничения доступа с полным контролем информационных потоков.

Использование отношения $\leq$ и операций sup**и**, inf**и** требует в практических системах переборно-циклических алгоритмов прохождения иерархического рубрикатора, что может вызывать повышенные вычислительные затраты. Альтернативой в подобных случаях может стать использование листовой тематической решетки, изоморфной решетке $\boldsymbol{\Lambda}_{\text{и}}(\boldsymbol{T}_{\text{и}\varnothing}, \leq, \sup\textbf{и}, \inf\textbf{и})$.

Введем следующее понятие.

Определение 2.3.12. Листовым тематическим множеством $\boldsymbol{T}^{\text{Л}}(\tau_i)$ вершины τ_i называется совокупность всех листовых вершин $\tau^{\text{Л}}_j$, подчиненных данной вершине тематического классификатора $\boldsymbol{T}_{\text{и}}$.

Отметим, что для листовой вершины $\tau^{\text{Л}}_j$ ее листовое тематическое множество $\boldsymbol{T}^{\text{Л}}(\tau_j)$ представляется одноэлементным множеством, единственный элемент которого совпадает с самой листовой вершиной.

На множестве листовых подмножеств $\boldsymbol{T}^{\text{Л}}$ как и на множестве **P** подмножеств любого множества отношение включения $\subseteq$ задает частичный порядок.

Справедливо следующее утверждение.

Лемма 2.3.1. Частично упорядоченное относительно отношения включения ⊆ множество листовых тематических множеств $\{\mathcal{T}^{Л}(\tau_1), \mathcal{T}^{Л}(\tau_2), \ldots, \mathcal{T}^{Л}(\tau_M)\}$ вершин иерархического рубрикатора изоморфно частично упорядоченному множеству тематических рубрик $\{\tau_1, \tau_2, \ldots \tau_M\}$, задаваемому иерархическим рубрикатором.

Лемма 2.3.2. Теоретико-множественное пересечение ∩ листовых множеств вершин иерархического рубрикатора $\mathcal{T}^{Л}(\tau_i) \cap \mathcal{T}^{Л}(\tau_j)$ эквивалентно операции взятия наибольшей нижней границы рубрик inf**и** $\{\tau_i, \tau_j\}$.

Для построения операции взятия наименьшей верхней границы листовых множеств, изоморфной операции sup**и**, введем следующее понятие.

Определение 2.3.13. Иерархическим объединением ∪**ил** листовых множеств $\mathcal{T}^{Л}(\tau_i)$, $\mathcal{T}^{Л}(\tau_j)$ будем называть листовое множество $\mathcal{T}^{Л}(\tau_k)$ вершины иерархического рубрикатора τ_k, являющейся ближайшим общим предком вершин τ_i и τ_j, порождающих соответствующие листовые множества.

Совершенно очевидно, что по самому определению 2.3.13 операция ∪**ил** эквивалентна операции sup**и**. Заметим также, что операции ∪**ил** и ∩ не выводят свои результаты за пределы множества $\mathcal{T}^{Л}$ листовых множеств вершин иерархического рубрикатора. Таким образом, на множестве $\mathcal{T}^{Л}$ имеем решетку $\Lambda_{и}$ ($\mathcal{T}^{Л}$, ⊆, ∪**ил**, ∩), изоморфную решетке $\Lambda_{и}$ ($\mathcal{T}_{и\varnothing}$, ≤, sup**и**, inf**и**).

Использование решетки листовых множеств $\Lambda_{и}$ ($\mathcal{T}^{Л}$, ⊆, ∪**ил**, ∩) позволяет применять единые механизмы тематического разграничения доступа в системах основанных на дескрипторной и иерархически монорубрицированной тематической классификации.

Для удобства рассмотрения решеток при мультирубрицированном подходе введем следующие понятия.

Определение 2.3.14. Иерархическим сжатием $\vee_{\text{и}}$ множества элементов $\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\}$ $(L < M)$, являющихся вершинами корневого дерева, задающего частичный порядок на множестве рубрик иерархического классификатора $T_{\text{и}}=\{\tau_1, \tau_2, \ldots, \tau_M\}$, будем называть операцию взятия ближайшей большей по иерархии дерева вершины τ_k в том и только в том случае, если множество $\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\}$ составляет полный набор вершин, непосредственно подчиненных вершине (родителю) τ_k .

Определение 2.3.15. Множество $I_{\text{Р}} \subseteq T_{\text{и}}$ будем называть рубрикаторным идеалом при выполнении двух условий:

1) если для любых $\tau \in T_{\text{и}}$ и $\tau' \in I_{\text{Р}}$ из $\tau \leq \tau'$ вытекает $\tau \in I_{\text{Р}}$, т. е. $I_{\text{Р}}$ является порядковым идеалом в корневом дереве рубрик;

2) если $\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\} \subseteq I_{\text{Р}}$ и $\vee_{\text{и}}\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\}=\tau_k$, то в состав множества $I_{\text{Р}}$ входит и $\tau_k \in I_{\text{Р}}$, где $L \leq M$.

Таким образом, рубрикаторный идеал является множеством вершин иерархического классификатора, которое замкнуто относительно операции взятия меньшего, т. е. является, по сути, объектом, называемым порядковым идеалом. Вместе с тем в отличие от классического порядкового идеала, он обязательно включает вершины-родители, при вхождении в идеал полного набора их сыновей. На рис. 2.18 представлены примеры рубрика- торных идеалов.

С содержательной точки зрения рубрикаторные идеалы представляют объекты, на которые согласно определению 2.3.9 при мультирубрицированной тематической классификации могут отображаться сущности КС (субъекты и объекты доступа), т. е. множество рубрик иерархического классификатора с обязательным наличием подчиненных вершин для каждой нелистовой вершины.

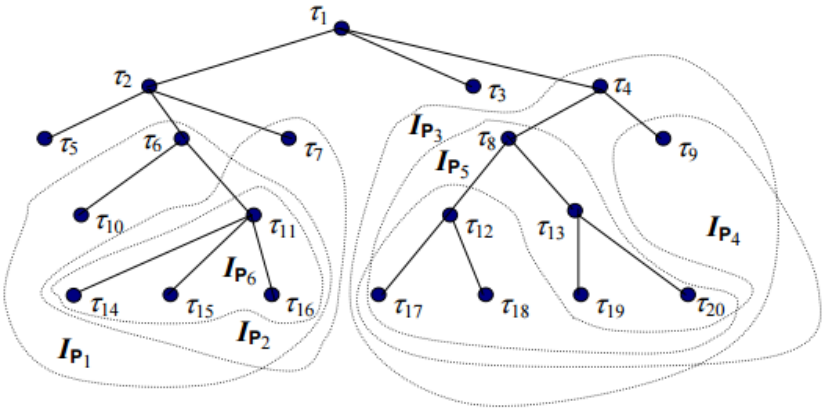

Рис. 2.18. Примеры рубрикаторных идеалов

Множество всех рубрикаторных идеалов, которые могут быть определены на корневом дереве рубрик (на иерархическом классификаторе) будем обозначать $\boldsymbol{I}_{\mathbf{P}}$.

Отношение включения $\subseteq$ одних рубрикаторных идеалов, являющихся подмножеством вершин корневого дерева рубрик, в другие рубрикаторные идеалы задает на множестве $\boldsymbol{I}_{\mathbf{P}}$ частичный порядок. Отметим также, что пустое множество по определению 2.3.15 является также рубрикаторным идеалом.

Очевидна справедливость следующего утверждения.

Лемма 2.3.3. Пересечение $\cap$ любых рубрикаторных идеалов корневого дерева рубрик является также рубрикаторным идеалом.

Вместе с тем, если рассматривать простое теоретико-множественное объединение $\cup$ рубрикаторных идеалов, то нетрудно заметить, что его результатом могут быть множества, в которых не выполняется второе условие определения 2.3.15. В частности, по примерам, представленным на рис. 2.18, не является рубрикаторным идеалом теоретико-множественное объединение рубрикаторных идеалов $\boldsymbol{I}_{\mathbf{P}_4}$ и $\boldsymbol{I}_{\mathbf{P}_5}$, так как не

содержит вершины τ_4, хотя включает полный набор ее сыновей $\{\tau_8, \tau_9\}$.

Основываясь на использовании понятия иерархического сжатия по определению 2.3.14, можно ввести специальную модификацию операции теоретико-множественного объединения для рубрикаторных идеалов – **Uир**.

Определение 2.3.16. Объединением **Uир** рубрикаторных идеалов $I_{P_i} \cup I_{P_j}$ будем называть их теоретико-множественное объединение, дополненное вершинами, полученными иерархическим сжатием подмножеств вершин, начиная с множества $I_{P_i} \cup I_{P_j}$.

Тогда справедливо следующее утверждение.

Лемма 2.3.4. Объединение **Uир** любых рубрикаторных идеалов корневого дерева рубрик является также рубрикаторным идеалом.

В качестве примера отметим, что по рубрикаторным идеалам имеем: $I_{P_6} = I_{P_1} \cap I_{P_2}$, а $I_{P_3} = I_{P_4} \cup_{ир} I_{P_5}$.

Из определения 2.3.15, лемм 2.3.3 и 2.3.4 вытекает важное следствие.

Следствие 2.3.4.1. Множество всех рубрикаторных идеалов дерева рубрик является решеткой $\Lambda_и(I_P, \subseteq, \cap, \cup_{ир})$ относительно теоретико-множественного включения $\subseteq$, операций теоретико-множественного пересечения $\cap$ и специальной операции (по определению 2.3.16) объединения **Uир**.

В результате имеем тематическую решетку, на базе которой можно строить модели тематического разграничения доступа при мультирубрицированной тематической классификации сущностей КС.

Вместе с тем на практике при мультирубрицированной классификации указываются только узловые тематические

рубрики без явного включения в тематику сущностей КС соответствующих подчиненных рубрик. Поэтому введем следующее понятие.

Определение 2.3.17. Мультирубрикой T^{M}_{i} называется любое под- множество $\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_L}\}$ $(L \le M)$ множества вершин корневого дерева, задающего частичный порядок на множестве $T_{и} = \{\tau_1, \tau_2, \ldots, \tau_M\}$ при выполнении следующих двух условий:

1) любая вершина τ_{i_k} несравнима с любой другой вершиной τ_{i_m} того же подмножества – $\tau_{i_k} \diamond \tau_{i_m}$, $k \neq m$;

2) в $\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_L}\}$ не содержится полного набора сыновей ни одной из вершин.

Множество всех мультирубрик на корневом дереве рубрик будем обозначать T^{M} $(T^{M} \in T^{M})$.

Покажем, что между рубрикаторными идеалами и мультирубриками имеется взаимно однозначное соответствие.

Для удобства введем несколько вспомогательных определений.

Определение 2.3.18. Порожденным (частичным порядком) множеством будем считать наименьшее множество, содержащее порождающее (исходное) множество и замкнутое относительно операции взятия меньшего.

Пусть **M** $\subseteq T_{и}$. Через < **M** > обозначим рубрикаторный идеал, порожденный множеством M, т. е. пересечение всех рубрикаторых идеалов, содержащих **M**. Ясно, что < **M** > является наименьшим рубрикаторным идеалом, содержащим **M**.

Определение 2.3.19. Элемент τ рубрикаторного идеала $I_{Р}$ будем называть максимальным, если для любого τ'$\in I_{Р}$ либо τ' $\le$ τ, либо τ' и τ несравнимы.

Обозначим через **A** множество всех максимальных элементов из рубрикаторного идеала I_P. Тогда очевидно, что **A** является порождающим множеством рубрикаторного идеала I_P. Заметим, далее, что также очевидно, что **A** состоит из попарно несравнимых элементов. Подобные подмножества будем называть антицепями (в отличие от цепей, образуемых множеством попарно сравнимых элементов).

Очевидна справедливость следующего утверждения.

Лемма 2.3.5. Антицепь, образуемая множеством всех максимальных элементов некоторого рубрикаторного идеала, является мультирубрикой, порождающей соответствующий рубрикаторный идеал.

Таким образом, имеется естественное взаимно однозначное соответствие между мультирубриками и рубрикаторными идеалами. Отметим, что пустой мультирубрике соответствует пустой рубрикаторный идеал. Кроме того, каждой рубрике отвечает одноэлементная мультирубрика, ее содержащая. Для удобства в дальнейшем одноэлементную мультирубрику будем отождествлять с ее единственной рубрикой.

Покажем далее, что на множестве мультирубрик можно построить решетку, эквивалентную решетке рубрикаторных идеалов $\Lambda_{и}(I_P, \subseteq, \cap, \cup_{ир})$.

С этой целью, прежде всего, введем понятие доминирования мульти- рубрик.

Определение 2.3.20. Мультирубрика τ^{M}_{i} доминирует над мульти- рубрикой $\tau^{M}_{j} - \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\} \le \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ в том и только в том случае, когда для любого m=1,…,J существует k=1,…,I такое, что $\tau_{j_m} \le \tau_{i_k}$ (вершина τ_{j_m} подчинена по корневому дереву вершине τ_{i_k}):

$$\forall\ \tau_{j_m} \in \tau^{M}_{j},\ \exists\ \tau_{i_k} \in \tau^{M}_{i},\ \tau_{j_m} \le \tau_{i_k}.$$

Легко проверить, что введенное отношение доминирования мультирубрик $\leq$ рефлексивно, транзитивно и антисимметрично, т. е. является отношением частичного порядка.

В частности, вернувшись еще раз к корневому дереву, можно привести следующие примеры доминирования мультирубрик:

$\{\tau_5, \tau_6\} \leq \{\tau_2, \tau_3\}$, $\{\tau_3, \tau_5, \tau_6\} \leq \{\tau_2, \tau_3\}$, $\{\tau_7, \tau_{11}\} \leq \{\tau_2, \tau_3\}$, $\{\tau_{13}, \tau_{17}\} \leq \{\tau_7, \tau_8\}$, $\{\tau_{12}, \tau_{19}\} \leq \{\tau_7, \tau_8\}$, $\{\tau_9, \tau_{10}, \tau_{13}, \tau_{14}, \tau_{16}, \tau_{18}\} \leq \{\tau_3, \tau_4, \tau_6\}$, $\{\tau_{11}, \tau_{12}, \tau_{19}\} \leq \{\tau_3, \tau_4, \tau_6\}$ и т.д.

Справедливо следующее утверждение.

Теорема 2.3.3. Частично упорядоченное относительно отношения включения $\subseteq$ множество рубрикаторных идеалов изоморфно частично упорядоченному по отношению доминирования $\leq$ множеству мультирубрик иерархического классификатора.

Определение 2.3.21. Объединением $\cup_{\text{м}}$ мультирубрик $\mathcal{T}^{\text{м}}{}_i = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ и $\mathcal{T}^{\text{м}}{}_j = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ называется операция формирования множества вершин иерархического рубрикатора $\mathcal{T}^{\text{м}\cup} = \mathcal{T}^{\text{м}}{}_i \cup_{\text{м}} \mathcal{T}^{\text{м}}{}_j$ на основе следующего алгоритма:

1) Формируется теоретико-множественное объединение множеств вершин, составляющих мультирубрики $\mathcal{T}^{\cup} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\} \cup \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$;

2) Формируется набор вершин $\mathcal{T}^{\text{м}\cup'}$ путем исключения из набора $\mathcal{T}^{\cup}$ тех вершин, которые доминируются хотя бы одной другой вершиной из того же набора $\mathcal{T}^{\cup}$ – $(\tau_k \in \mathcal{T}^{\cup} \wedge \tau_k \notin \mathcal{T}^{\text{м}\cup}) \equiv (\exists\ \tau_m \in \mathcal{T}^{\cup} \wedge \tau_m \leq \tau_k \wedge \tau_m \neq \tau_k)$;

3) Формируется итоговый набор вершин $\mathcal{T}^{\cup}$ путем добавления в набор $\mathcal{T}^{\text{м}\cup'}$ результатов иерархического сжатия по всем подмножествам набора вершин $\mathcal{T}^{\text{м}\cup'}$ и одновременным

исключением соответствующих наборов сыновей при непустом результате сжатия.

Иными словами – для построения мультирубрики, являющейся объединением двух мультирубрик, необходимо в теоретико-множественном объединении исходных мультирубрик оставить максимальные (определение 2.3.19) элементы и произвести при необходимости иерархические сжатия.

Справедливо следующее утверждение.

Лемма 2.3.6. Множество рубрик $\mathcal{T}^{\mathcal{M}\cup} = \mathcal{T}^{\mathcal{M}}_i \cup_{\mathcal{M}} \mathcal{T}^{\mathcal{M}}_j$, формируемое на основе объединения мультирубрик,

a) является мультирубрикой;

b) доминирует над мультирубриками

$$\mathcal{T}^{\mathcal{M}}_i \ и \ \mathcal{T}^{\mathcal{M}}_j, \ т.е. \ \mathcal{T}^{\mathcal{M}}_i \le \mathcal{T}^{\mathcal{M}\cup} \wedge \mathcal{T}^{\mathcal{M}}_j \le \mathcal{T}^{\mathcal{M}\cup};$$

c) является наименьшей верхней границей мультирубрик $\mathcal{T}^{\mathcal{M}}_i$ и $\mathcal{T}^{\mathcal{M}}_j$.

Определение 2.3.22. Пересечением $\cap_{\mathcal{M}}$ мультирубрик $\mathcal{T}^{\mathcal{M}}_i = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ и $\mathcal{T}^{\mathcal{M}}_j = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ называется операция формирования множества вершин иерархического рубрикатора $\mathcal{T}^{\mathcal{M}\cap} = \mathcal{T}^{\mathcal{M}}_i \cap_{\mathcal{M}} \mathcal{T}^{\mathcal{M}}_j$ на основе следующего алгоритма:

1) Из множества вершин мультирубрики $\mathcal{T}^{\mathcal{M}}_i = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ формируется множество вершин $\mathcal{T}^{\mathcal{M}'}_i$, которые доминируются хотя бы одной вершиной из множества вершин другой мультирубрики $\mathcal{T}^{\mathcal{M}}_j = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$;

2) Из множества вершин мультирубрики $\mathcal{T}^{\mathcal{M}}_j = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ формируется множество вершин $\mathcal{T}^{\mathcal{M}'}_j$, которые доминируются хотя бы одной вершиной из множества вершин первой мультирубрики $\mathcal{T}^{\mathcal{M}}_i = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$;

3) Формируется теоретико-множественное объединение

$$T^{M\cap} = T^{M}{}_{i} \cup T^{M}{}_{j}.$$

Покажем справедливость следующего утверждения.

Лемма 2.3.7. Множество рубрик $T^{M\cap} = T^{M}{}_{i} \cap_{M} T^{M}{}_{j}$, формируемое на основе пересечения мультирубрик,

a) является мультирубрикой;

b) доминируется мультирубриками $T^{M}{}_{i}$ и $T^{M}{}_{j}$, т. е

$$T^{M\cap} \le T^{M}{}_{i} \wedge$$
$$T^{M\cap} \le T^{M}{}_{j};$$

c) является наименьшей нижний границей мультирубрик $T^{M}{}_{i}$ и $T^{M}{}_{j}$.

2.3.3. Модель тематико-иерархического разграничения доступа

Основные положения модели сводятся к следующему.

1. Информационно-логическая схема предметной области системы представляется тематическим иерархическим классификатором (рубрикатором).

Рубрикатор включает конечное множество тематических рубрик $T_{и} = \{\tau_1, \tau_2, \ldots, \tau_M\}$, на котором установлен частичный порядок, задаваемый корневым деревом.

2. Множество сущностей системы **X = S ∪ O** тематически классифицируется на основе отображения на множество мультирубрик T^{M}, определенных на корневом дереве иерархического рубрикатора.

В рамках мультирубрицированного отображения $F_{и2}[x]$ сущностей КС на иерархический рубрикатор будем считать, что существует функция тематического окрашивания f_{M}, которая в каждый момент времени для любой сущности

системы **x** ∈ **X** определяет соответствующую ей мультирубрику: $f_M[x] = T^M_i$, где

$$x \in S \cup O,\ T^M_i \in T^M.$$

3. Функционирование системы сопровождается переходами из одного состояния (момент времени tk) в другое состояние (момент времени t_{k+1}). В результате перехода в системе возникают новые отношения доступа (новые потоки) между существующими сущностями (**X = S ∪ O**), либо возникают/удаляются новые сущности – субъекты и объекты доступа.

В дальнейшем ограничимся двумя видами потоков – на запись (**w**) в объект и на чтение (**r**) из объекта, представленных на рис. 2.19.

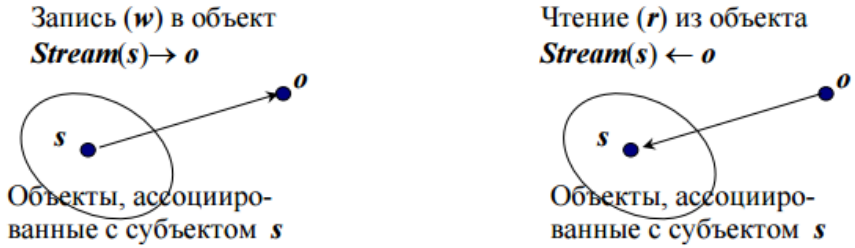

Рис. 2.19. Потоки на запись и чтение

Множество потоков обладает свойством транзитивности. В частности, с точки зрения безопасности чтение субъектом s_m из одного объекта o_i и запись в другой объект o_j и, далее, чтение другим субъектом s_n из объекта o_j и запись в объект o_k тождественно потоку из информации объекта o_i в объект o_k через субъекты s_m и s_n – $Stream(s_m, s_n, o_i, o_j) \rightarrow o_k$.

С учетом понятия субъекта и объекта доступа (определения 1.3.2, 1.3.3), источника для субъекта доступа (определение 1.3.4), объектов, ассоциированных с субъектом доступа (определение 1.3.5), процессы порождения субъектов и

объектов доступа будем определять потоками, представленными на рис. 2.20.

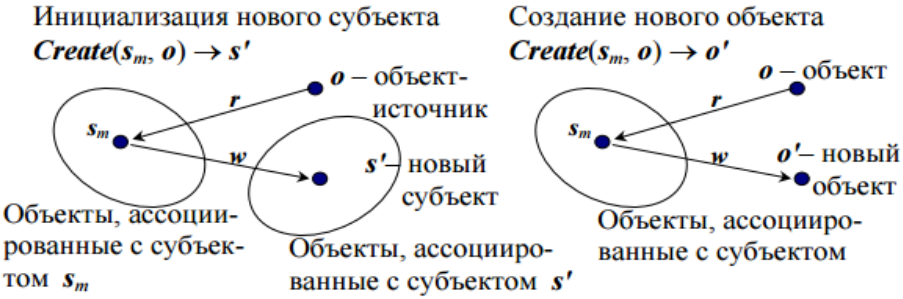

Рис. 2.20. Потоки при создании субъектов и объектов доступа

Таким образом, переходы системы, сопровождающиеся созданием новых объектов или субъектов доступа, описываются, как и переходы, вызываемые доступами существующих субъектов к существующим объектам, также двумя видами потоков – на чтение и на запись.

Проблема разграничения (безопасности) доступа заключается в синтезе таких механизмов принятия решения о правомочности доступа субъектов к объектам, при которых с учетом транзитивности потоков реализуется некоторое подмножество безопасных по определенному критерию потоков.

4. На основе анализа сущности мультирубрицированной тематической классификации и с целью конкретизации общего критерия безопасности тематического доступа по определению 2.3.2, сформулируем следующий очевидный критерий безопасности для системы **ΣТии**.

Определение 2.3.23. **Система безопасна** тогда и только тогда, когда в ней отсутствуют потоки следующих видов:

- от сущностей с более широкой тематикой к сущностям с более узкой тематикой;
- между несравнимыми по тематике сущностями.

5. Переходы системы, обусловленные запросами и осуществлением доступов существующих субъектов к существующим объектам, санкционируются монитором безопасности объектов на основе следующих правил, вытекающих из критерия, задаваемого определением 2.3.23.

Правило 2.3.1. Доступ субъекта s к объекту o, вызывающий поток по чтению **Stream(s)←o**, неопасен и может быть **МБО** разрешен тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта: $f_м[s] \geq f_м[o]$.

Правило 2.3.2. Доступ субъекта s к объекту o, вызывающий поток по записи **Stream(s)→o**, неопасен и может быть **МБО** разрешен тогда и только тогда, когда мультирубрика объекта доминирует над мульти- рубрикой субъекта: $f_м[o] \geq f_м[s]$.

Из правила 2.3.2 следует, что при создании нового объекта **o' МБО** должен присвоить ему мультирубрику, тождественную или более широкую, чем мультирубрика субъекта, осуществляющего операцию создания объекта - $f_м[o'] \geq f_м[s]$. Данная процедура может быть полностью автоматизирована (строгий принцип) или осуществляться на основе специальных запросов пользователю (нестрогий принцип). При строгом принципе **МБО** присваивает новому объекту мультирубрику субъекта. При нестрогом принципе **МБО** на основе специального запроса к пользователю может присвоить новому объекту любую мультирубрику, доминирующую (более широкую) над мультирубрикой субъекта.

6. Переходы системы, связанные с порождением новых объектов и субъектов доступа, санкционируются **МБО** и **МБС** на основе следующих правил.

Правило 2.3.3. Порождение субъектом **s** нового объекта **o'**, в том числе и за счет чтения из другого объекта о, неопасно и может быть **МБО** разрешено тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта **o**, при этом **МБО** присваивает новому объекту **o'** мультирубрику, доминирующую над мультирубрикой субъекта: $f_м[o] \le f_м[s] \le f_м[o']$.

При инициализации нового субъекта доступа ситуация иная. Исходя из аксиоматического предположения, монитор безопасности субъектов реализует следующее правило (аналогичное соответствующим правилам в моделях **ΣТдс и ΣТднс**).

Правило 2.3.4. Инициализация субъектом **s** нового субъекта **s'** посредством воздействия на объект источник **o** неопасна и может быть **МБС** разрешена тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта-источника, при этом **МБС** присваивает новому субъекту мультирубрику, тождественную мультирубрике инициализирующего субъекта:
$f_м[o] \le f_м[s] \equiv f_м[s']$.

7. В системе коллективного доступа помимо потоков, вызываемых одиночными доступами (один субъект к одному объекту), могут существовать потоки, вызываемые множественными доступами (один субъект одновременно к нескольким объектам, несколько субъектов одновременно к одному объекту).

Санкционирование подобных потоков осуществляется на основе следующего правила.

Правило 2.3.5. Одновременный множественный доступ субъекта s к объектам $o_1, o_2, \dots$ или субъектов $s_1, s_2, \dots$ к объекту о может быть разрешен (неопасен) тогда и только тогда, когда каждый одиночный доступ из запрашиваемой совокупности доступов, образующих множественный доступ, удовлетворяет правилам 2.3.1,2.3.2,2.3.3 и 2.3.4.

Правило 2.3.5 вытекает из транзитивности множества потоков, а также участия в потоках информации объектов, ассоциированных с субъектами доступа, что с точки зрения безопасности обусловливает эквивалентность последовательности одиночных потоков и соответствующего множественного доступа. Кроме того, отметим, что это правило распространяется, в том числе, и на процессы порождения новых объектов и инициализации новых субъектов доступа.

Справедливо следующее утверждение.

Теорема 2.3.4. В системе с отображением множества субъектов и объектов доступа на множество тематических мультирубрик, в которой доступы санкционируются по правилам 2.3.1, 2.3.2, 2.3.3, 2.3.4 и 2.3.5, реализуется множество только таких потоков, которые удовлетворяют критерию безопасности по определению 2.3.23.

2.4. Модели безопасности на основе ролевой политики

2.4.1. Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений

В основе рассмотренных ранее политик безопасности лежат отношения между отдельным пользователем (субъектом) и объектом доступа, определяемые либо внешним фактором (дискреционный доступ), либо уровнем безопасности (мандатный доступ), либо тематикой информации (тематический доступ).

Вместе с тем, анализ различных организационно-управленческих и организационно-технологических схем, показывает, что в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как определенную роль, представляет некоторую абстрактную,

точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий.

Еще одним аспектом реальных организационно-технологических и управленческих схем является использование понятий прав и полномочий, как неких процедур над ресурсами системы, отражающих организационно-технологические процессы предметной области КС. Иначе говоря, права и полномочия сотрудникам по их должностям предоставляются не на уровне элементарных операций над ресурсами (читать, изменять, добавлять, удалять, создавать), а на уровне совокупностей элементарных операций, сгруппированных в отдельные логически обобщенные процедуры обработки информации (например, кредитные или дебетные операции над определенными бюджетами).

Таким образом, политика разграничения доступа в компьютерных системах, автоматизирующих те или иные организационно-технологические или организационно-управленческие процессы, должна строиться на основе функционально-ролевых отношений, складывающихся в предметной области КС.

Впервые подобный подход был рассмотрен в конце 70-х – начале 80-х годах в исследованиях по процессам разграничения доступа корпорации IBM и получил название ролевого управления доступом. В начале 80-х годов была представлена модель Лендвера-МакЛина, встречающаяся в литературе также под названием **MMS**-модели, сочетающая дискреционный и мандатный принципы разграничения доступа с использованием понятия и механизма ролей. Несколько позже появились и формальные выражения ролевых основ управления доступом (Role-Based Access Control –**RBAC**).

Основой ролевых моделей, как отмечалось, является введение в субъектно-объектную модель КС дополнительной категории активных сущностей – ролей. Можно дать следующее формальное определение роли.

Определение 2.4.1. Ролью называется активно действующая в КС абстрактная сущность, обладающая логически взаимосвязанным набором полномочий, необходимых для выполнения определенных функциональных обязанностей пользователями системы.

Полномочия, как уже отмечалось, трактуются, как право осуществлять некоторые функционально-логические процедуры над всей совокупностью объектов системы или над определенной их группой. При этом, однако, в известных формальных ролевых моделях не вводятся отдельные механизмы спецификации полномочий, а используется традиционный набор элементарных методов доступа (чтение, запись, и т. д.). В то же время в таких широко распространенных разновидностях систем, как СУБД, подобные спецификации функционально-логических процедур над данными используются повсеместно. Основу обработки данных в реляционных СУБД составляют запросы, обособляющие в отдельные именованные сущности операции над данными (инструкции SELECT, INSERT, UPDATE, DELETE), объекты данных (таблицы) и результаты обработки. Сконструированные и выраженные на языке SQL запросы хранятся в БД вместе с данными и составляют отдельную группу объектов (сущностей) базы данных. Пользователям системы предоставляются права запускать определенные запросы, что можно интерпретировать как дискреционный способ предоставления полномочий по обработке данных.

В операционных системах, ввиду их большей универсальности и ориентированности на самый широкий круг предметных областей, полномочия ролей (например, для ролей администраторов, аудиторов, или полномочия для рабочих

групп пользователей) определяются чаще всего на основе дискреционного принципа через права по определенным методам доступа к определенным объектам системы или к объектам отдельных категорий (к спискам доступа, к журналу аудита и т. д.). Подобный подход называют механизмом привилегий.

Введение ролей приводит к двухэтапной организации системы разграничения доступа:

1. Создание ролей и определение их полномочий (прав доступа к объектам);

2. Назначение ролей пользователям системы.

Соответственно формальные спецификации ролевых моделей должны регламентировать тем или иным способом, точнее в рамках той или иной политики, и определение полномочий ролям и назначение ролей пользователям.

Управление доступом в ролевых системах требует разбиения процесса функционирования системы и работы пользователя на сеансы, в каждом из которых, в свою очередь, выделяется две фазы:

1. Авторизация в данном сеансе пользователя с одной или несколькими разрешенными (назначенными на втором этапе организации доступа) для него ролями;

2. Разрешение или запрещение субъектам пользователя доступа к объектам системы в рамках полномочий соответствующих ролей, с которыми авторизован в данном сеансе пользователь.

Нетрудно увидеть, что ролевые модели сочетают мандатный подход к организации доступа через определенную агрегацию субъектов и объектов доступа, и тем самым обеспечивают жесткость правил разграничения доступа, и дискреционный подход, обеспечивающий гибкость в настройке системы разграничения доступа на конкретные функционально-организационные процессы предметной области КС. Данные особенности ролевой политики позволяют строить системы разграничения доступа с хорошей управляемостью в сложных системах с большим количеством

пользователей и объектов, и поэтому находят широкое применение в практических системах.

2.4.2. Формальная спецификация и разновидности ролевых моделей

Приведем формальную спецификацию ролевой модели разграничения доступа.

1. КС представляется совокупностью следующих множеств:

- множества пользователей **U**;
- множества ролей $\mathfrak{R}$;
- множества полномочий **P**;
- множества сеансов **C** работы пользователей с системой.

Множество полномочий **P** в общем виде задается специальными механизмами, объединяющими операции доступа и объекты доступа, например, запросами на обработку данных в СУБД, или иными именованными процедурами обработки данных, в том числе возможно высокого логического уровня.

2. Ролевые отношения устанавливаются следующими отображениями множеств сущностей системы:

FP$\mathfrak{R}$: P x $\mathfrak{R}$ – отображение множества полномочий на множество ролей;

FU$\mathfrak{R}$: U x $\mathfrak{R}$ – отображение множества пользователей на множество ролей.

Нетрудно видеть, что отображения **FP$\mathfrak{R}$** и **FU$\mathfrak{R}$** обеспечивают первый и второй этапы процессов организации системы ролевого доступа. При этом отображение **FU$\mathfrak{R}$** может реализовываться механизмами одной из базовых политик разграничения доступа – матрицей «Пользователи-Роли», или на основе соотношения степеней допуска пользователей и грифов конфиденциальности ролей, или на основе соотношения разрешенных тематик пользователей и тематики ролей.

3. Управление доступом в системе осуществляется на основе введения следующих функций:

fuser**: C→ U** – значением функции **u=f**user**(c)** является пользователь **u ∈ U**, осуществляющий данный сеанс с работы с системой;

froles**: C→ R** – значением функции **R = f**roles**(c)** является набор ролей **R ⊆ ℜ** из доступных пользователю, по которым пользователь работает (осуществляет доступ) в данном сеансе **c ∈ C**;

fpermissions**: C→ P** – значением функции **P = f**permissions**(c)** является набор полномочий **P ⊆ P**, доступных по всем ролям, задействованным пользователем в данном сеансе **c ∈ C**;

4. Основное правило (критерий безопасности) ролевого доступа определяется следующим образом.

Правило 2.4.1. Система функционирует безопасно, если и только если любой пользователь **u ∈ U**, работающий в сеансе **c ∈ C**, может осуществлять действия (операции, процедуры) в рамках полномочия **p ∈ P**, при условии: **p∈ P**, где **P = f**permissions**(c).**

Нетрудно видеть, что основной акцент в процессах организации и управления доступом при ролевой политике заключается в особенностях отображения множества пользователей на множество ролей **FUℜ** и ограничений, накладываемых на функцию авторизации **f**roles**(c)** пользователя в данном сеансе с разрешенными ему отношением **FUℜ** ролями. Выражаясь предметным языком, можно так сформулировать основные вопросы организации ролевого доступа:

Сколько и каких ролей может быть назначено для работы с системой одному пользователю?

Сколько и какие роли может одновременно задействовать один пользователь в одном сеансе работы с системой?

Еще одним существенным обстоятельством являются возможные отношения между ролями, в том, числе возможная передача (делегирование) полномочий и прав от одних ролей другим ролям.

В зависимости от особенностей разрешения данных вопросов выделяют несколько разновидностей ролевых моделей:

• с иерархической организацией системы ролей;

• с взаимоисключающими на любые (все) сеансы ролями (модель статического распределения обязанностей);

• с взаимоисключающими на один сеанс ролями (модель динамического распределения обязанностей);

• с количественными ограничениями по ролям;

• с группированием ролей и полномочий.

Приведем краткую характеристику указанных разновидностей ролей.

Иерархическая система ролей

Данная разновидность ролевых моделей является наиболее близкой к реальным организационно-технологическим и организационно-управленческим схемам на предприятиях и в организациях. Должности сотрудников предприятий, организаций в большинстве случаев образуют иерархически подчиненные структуры. На рис. 2.21 представлены примеры иерархической системы ролей-должностей.

При этом помимо управленческого аспекта подчиненность ролей в большинстве случаев включает наследование прав и полномочий. В иерархически организованных структурах возможны два направления наследования полномочий и прав – «снизу» и «сверху».

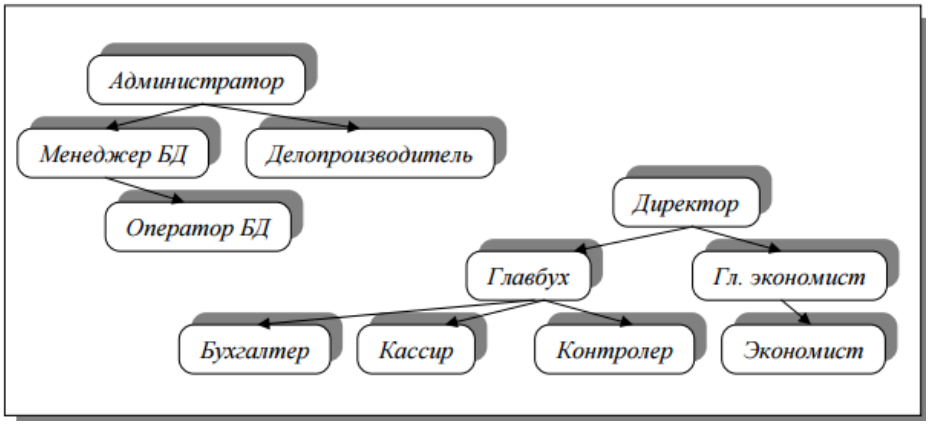

Рис. 2.21. Примеры иерархической организации системы должностей (ролей)

При наследовании «сверху» подчиненный субъект помимо своих индивидуальных (так называемых явных) прав и полномочий получает (наследует) права и полномочия родителей. Подобный подход широко применяется в организации доступа к объектам, образующим иерархически организованную структуру, а также в системах индивидуально-группового доступа.

Модели с иерархически организованными ролями основаны на механизме наследования «снизу», при котором старшая в иерархии роль получает (владеет) права и полномочия непосредственно подчиненных ролей и т. д.

С формальной точки зрения модель с иерархической системой ролей включает введение дополнительных и уточнение исходных отношений сущностей и функций системы –

FRR: $\mathfrak{R}$ x $\mathfrak{R}$ – отношение частичного порядка на множестве ролей, определяющее иерархию (подчиненность) ролей и задающее оператор доминирования ролей ≥, такое что: если для **$\rho 1, \rho 2 \in \mathfrak{R}$, $\rho 1 \geq \rho 2$**, то **$\rho 1$** находится в иерархии ролей выше, чем **$\rho 2$**;

$\mathcal{F}^{h}_{U\mathfrak{R}}: U \times \mathfrak{R}$ – отображение множества пользователей на множество ролей, причем вместе с каждой ролью **ρ** из набора назначенных для пользователя ролей, в него включаются и все роли **ρ '**, подчиненные **ρ**:

для $\forall \rho, \rho' \in \mathfrak{R}, u \in U: \rho \geq \rho' \wedge (u,\rho) \in \mathcal{F}^{h}_{U\mathfrak{R}}(u) \Rightarrow (u,\rho') \in \mathcal{F}^{h}_{U\mathfrak{R}}(u)$;

f^{h}_{roles}**: C→ R** – значением функции является набор ролей **R ⊆ ℜ**, из доступных пользователю, по которым пользователь работает (осуществляет доступ) в данном сеансе **c ∈ C**, с учетом иерархически подчиненных ролей:

$$f^{h}_{roles}(c) \subseteq \{\rho_i \mid (\exists\, \rho' \geq \rho_i\ (f_{user}(c), \rho') \in \mathcal{F}^{h}_{U\mathfrak{R}}(u))\}\ ;$$

$f^{h}_{permissions}$**: C→ P** – значением функции $\mathcal{P} = f^{h}_{permissions}(c)$ является совокупность полномочий **P ⊆ P**, доступных по всем ролям $\mathcal{R} = f^{h}_{roles}(c)$, задействованным пользователем в данном сеансе **c ∈ C** (с учетом полномочий подчиненных ролей).

В плане критического анализа модели с иерархической организацией системы ролей отметим, что в более строгом смысле необходимо регламентировать возможные типы отношений **FPℜ**, т. е. особенности отображения множества полномочий на множество иерархически организованных ролей. В частности, принципиальное значение имеет вопрос о теоретико-множественном соотношении полномочий старшей роли и ролей, непосредственно ей подчиненных. Другим принципиальным вопросом в этом же плане является возможность или невозможность назначения одного и того же полномочия одновременно двум ролям, находящимся в иерархическом подчинении.

Анализируя особенности прав и полномочий соподчиненных должностей в реальных организационно-управленческих схемах, можно предложить три подхода к структуре отношения FPℜ в системе с иерархически организованной системой ролей:

- строго таксономический листовой подход;
- не таксономический листовой подход;

• иерархически охватный подход.

При строго таксономическом листовом подходе все множество полномочий разбивается на непересекающиеся подмножества, назначаемые отношением **FP**ℜ листовым ролям корневого графа иерархии ролей (см. рис. 2.22):

$$\mathcal{F}^{h}{}_{P\Re}(\rho^{\Pi}_{j}) = \{p_{j_1}, p_{j_2}, \dots\},$$

$$\mathcal{F}^{h}{}_{P\Re}(\rho^{\Pi}_{j}) \cap \mathcal{F}^{h}{}_{P\Re}(\rho^{\Pi}_{i}) \cap \dots = \varnothing,$$

$$\mathcal{F}^{h}{}_{P\Re}(\rho^{\Pi}_{j}) \cup \mathcal{F}^{h}{}_{P\Re}(\rho^{\Pi}_{i}) \cup \dots = P.$$

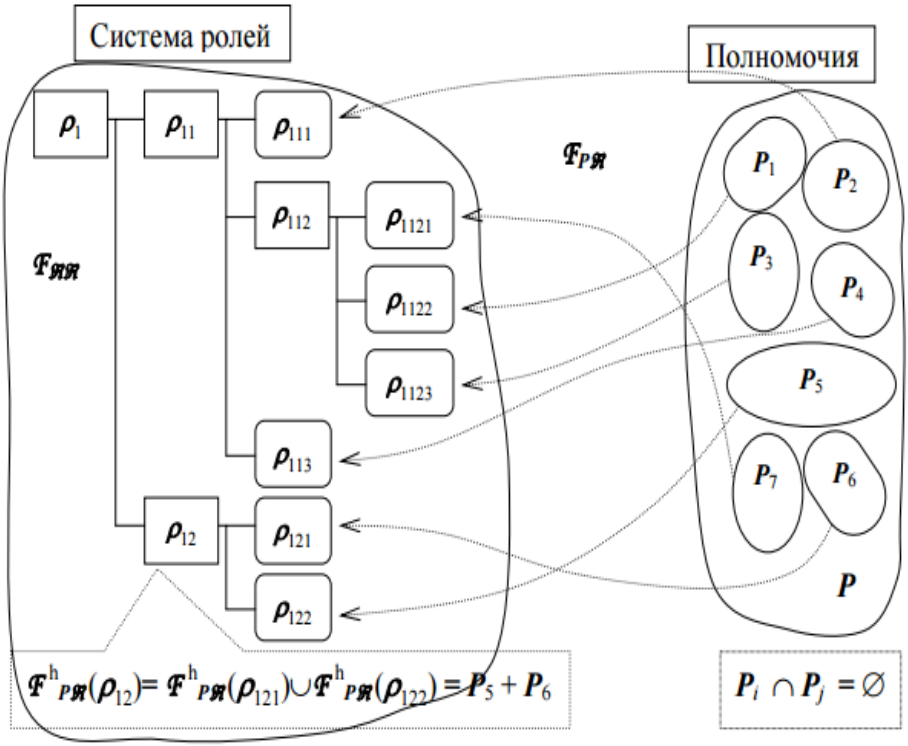

Рис. 2.22. Пример таксономического листового подхода к назначению полномочий в иерархической системе ролей

Полномочия старших ролей, т. е. ролей, которым соответствуют внутренние вершины корневого графа иерархии ролей, определяются как объединение прав и полномочий непосредственно подчиненных ролей, которым в графе иерархии ролей соответствуют вершины-сыновья:

$\mathcal{F}^{h}_{PR}(\rho^{И}_{k}) = \mathcal{F}^{h}_{PR}(\rho_{k_i}) \cup \mathcal{F}^{h}_{PR}(\rho_{k_j}) \cup \dots$, где $\{\rho_{k_i}, \rho_{k_j}, \dots\}$ – полный набор ролей-сыновей для роли $\rho^{И}_{k}$.

При нетаксономическом листовом подходе права и полномочия непосредственно получают также только листовые роли. Полномочия старших ролей также образуются объединением полномочий непосредственно подчиненных ролей. При этом, однако, пересечение наборов полномочий листовых ролей-братьев, т. е. подчиненных общей старшей роли, может быть не пустым: $\mathcal{F}^{h}_{PR}(\rho^{П}_{j}) \cap \mathcal{F}^{h}_{PR}(\rho^{П}_{i}) \cap \dots \neq \varnothing$.

Нетрудно видеть, что подобный подход в отличие от строго таксономического не обеспечивает автоматического наделения корневой в иерархии роли полным набором полномочий системы.

При иерархически охватном подходе в набор прав и полномочий старших ролей непосредственно включаются только те права и полномочия, которые не вошли в наборы прав и полномочий подчиненных ролей:

$$\mathcal{F}^{h}_{PR}(\rho_k) = \{p_{k_1}, p_{k_2}, \dots\},$$

$$\mathcal{F}^{h}_{PR}(\rho^{И}_{k}) \cap \mathcal{F}^{h}_{PR}(\rho_i) = \varnothing,$$

где $\{\rho^{И}_{k} \geq \rho_i\}$.

При этом в соответствии с функциями f^{h}_{roles} и $f^{h}_{permissions}$ при иерархически охватном подходе итоговый набор полномочий пользователя, задействовавшего в сеансе с старшую роль $\rho^{И}_{k}$, включает набор прав и полномочий всех ролей, подчиненных роли $\rho^{И}_{k}$.

Таксономический листовой подход отражает те предметные области, для которых набор полномочий (прав) рассматривается как общий ресурс, распределяемый между низовыми звеньями системы, к примеру, сельскохозяйственные земельные угодья, наделяемые крепостным крестьянам, из совокупности наделов которых складываются владения феодалов. Другой пример – структуры со строгой организационно-управленческой вертикалью – право руководить рядовыми сотрудниками имеют только их непосредственные руководители (низшее управленческое звено); руководители более высокого управленческого уровня право непосредственного руководства рядовыми сотрудниками получают на основе объединения соответствующих прав подчиненных руководителей более низкого управленческого звена.

Второй подход идеологически сходен с первым, за исключением того, что конкретное право, полномочие может предоставляться не одной листовой роли, а сразу нескольким.

Иерархически охватный подход отражает более сложные, но и более распространенные предметные области, в которых на множестве прав и полномочий, в свою очередь, может быть задано отношение частичного порядка, что приводит к тому, что часть полномочий может быть присвоена ролям только определенного уровня иерархии. В подобных системах старшей роли (должности) непосредственно назначаются только права и полномочия соответствующего уровня иерархии, а права и полномочия подчиненных ролей наследуются и применяются автоматически.

Взаимоисключающие роли (статическое распределение обязанностей)

Особенностью некоторых предметных областей является запрет на предоставление определенного набора прав или полномочий в совокупности одному работнику. Подобные ограничения призваны усилить безопасность путем уменьшения вероятности злоумышленных действий по

наборам некоторых связанных критических процессов и процедур. Если данные процедуры могут выполняться только разными работниками, то для осуществления злоумышленных действий потребуется сговор соответствующих работников. Вероятность подобного (злоумышленного) развития ситуации в случае, когда все соответствующие права и полномочия имеет один человек существенно выше.

В формальном плане данный подход требует отображения множества ролей на множество подмножеств «несовместимых» ролей. При реализации подобного подхода положения и спецификации ролевой модели дополняются специальной функцией **f**exclusive**(ρ)**, которая для каждой роли задает набор несовместимых с ней ролей.

С учетом возможной несовместимости ролей на отображение **FUℜ**: накладывается следующее ограничение: если **(u, ρ) ∈ FUℜ (u) ∧ ρ'∈ f**exclusive**(ρ) ⇒ (u, ρ') ∉ FUℜ (u)**.

Если трактовать роль пользователя в КС как аналог служебной должности, то вырожденным, но повсеместно распространенным вариантом данного подхода является запрет назначения одному пользователю более двух ролей (нельзя исполнять сразу две должности по основному месту работы на постоянной основе).

Заметим также, что с формальной точки зрения запрет назначения пользователям взаимоисключающих ролей касается не собственно пользователей, а их учетных записей в КС. В результате часть элементов контрольно-ограничительных процедур в данной модели лежит вне компьютерной сферы, в частности, в запрете одному пользователю иметь несколько различных учетных записей в КС.

Взаимоисключающие роли (динамическое распределение обязанностей)

Во многих организационно-управленческих и организационно- технологических структурах работникам приходится совмещать выполнение определенных групп обязанностей или подменять других работников на

определенное время. В этом случае распределение функциональных или служебных обязанностей имеет динамический характер и организуется, скажем, на каждый конкретный рабочий день, смену или иной временной управленческо-технологический период. При этом часть полномочий, групп процедур также может иметь критический с точки зрения безопасности характер в плане одновременного их выполнения одним работником.

В ролевой модели для разрешения подобных критических ситуаций может применяться механизм взаимоисключающих на один сеанс ролей. Как и в предыдущем случае, множество ролей отображается на множество подмножеств «несовместимых» ролей на основе использования функции **f**exclusive**(ρ)**. При этом, однако, каких-либо ограничений на отношение **FU**$\mathfrak{R}$, т. е. запретов на назначение ролей одному пользователю, в том числе, и взаимоисключающих ролей, не накладывается.

Решение проблемы безопасности осуществляется через запрет на задействование в одном сеансе одним пользователем сразу нескольких взаимоисключающих ролей, скажем одновременно роли кассира-оператора и контролера-аудитора в финансовых процедурах. В формальном плане подобные ограничения обеспечиваются функцией froles, которая в каждом сеансе для конкретного пользователя задает активизированный им набор ролей с учетом ограничений на взаимоисключающие роли:

$$\forall\ \boldsymbol{\rho 1, \rho 2} \in \mathfrak{R}, \boldsymbol{\rho 1} \in \mathbf{f}\text{roles}\mathbf{(c)} \wedge \boldsymbol{\rho 2} \in \mathbf{f}\text{exclusive}\mathbf{(\rho 1)} \Rightarrow \boldsymbol{\rho 2} \notin \mathbf{f}\text{roles}\mathbf{(c)}.$$

В качестве примера подобного подхода отметим повсеместно практикуемый запрет на одновременное использование в одном сеансе работы с КС ролей «администратора» и «аудитора безопасности» в КС.

Ролевой метод динамического распределения обязанностей при правильной организации ролей относительно включения в них процедур, вызывающих те или иные информационные потоки, может в значительной степени усилить мандатные модели разграничения доступа. В

частности, таким образом можно организовать контроль и исключение некоторых потенциально опасных ситуаций, например, осуществление доступа к ценной (категорированной) информации и одновременный запуск недоверенных программ и процессов.

Количественные ограничения по ролям

Отдельным направлением идеологии исключения потенциально опасных ситуаций, связанных с набором критических по отношению к безопасности системы прав и полномочий, является возможность наложения количественных ограничений на права и полномочия, агрегируемые одной отдельно взятой ролью. В этом случае ограничения вводятся на отношение **FP$\mathfrak{R}$** через введение функции $f^{P}_{\text{cardinality}}: P \to N$, определяющей для каждой роли количество включенных в нее прав и полномочий:

$$\text{для } \forall\, p_k \mid \{\rho_m \mid (p_k, \rho_m) \in F_{P\mathfrak{R}}(p_k)\}\mid \le f^{P}_{\text{cardinality}}(p_k).$$

В других ситуациях требуется предоставление определенных полномочий как можно меньшему или строго ограниченному количеству сотрудников, скажем допуск к определенным опасным работам, право ознакомления с определенной информацией и т. п. Для реализации подобных ограничений в ролевой модели вводится функция $f^{\rho}_{\text{cardinality}}: \mathfrak{R} \to N$, определяющая число пользователей, получивших назначения на данную роль, и на этой основе устанавливаются ограничение на отношение **FU$\mathfrak{R}$**:

$$\text{для } \forall\, \rho_k \mid \{u_m \mid (\rho_k, u_m) \in F_{U\mathfrak{R}}(u_m)\}\mid \le f^{\rho}_{\text{cardinality}}(\rho_k).$$

Количественные ограничения могут в значительной степени облегчить администрирование систем, где требуется особо тщательный контроль за распределением прав и ответственности в коллективе пользователей.

Группирование ролей и полномочий

В некотором смысле противоположным по отношению к количественным ограничениям является группирование ролей и полномочий.

По смыслу и определению роль представляет группирование прав и полномочий в отдельную логически обособленную их совокупность, имеющую самостоятельное значение в предметной области КС. Поэтому, прежде всего, устанавливается механизм, контролирующий агрегирование в одну роль некоторых логически связанных прав и полномочий. Для этого на множестве полномочий **P** вводится функция $f^{p}_{\text{prerequisite}}: P \to \mathcal{P}$, устанавливающая для каждого права (полномочия) **p** набор **P** ⊆ **P** логически связанных прав и полномочий, и введение следующего ограничения на отношение **FP$\mathfrak{R}$**: для $\forall (p, \rho) \in F_{P\mathfrak{R}}(p) \wedge p' \in f^{p}_{\text{prerequisite}}(p) \Rightarrow (p', \rho) \in F_{P\mathfrak{R}}(p)$.

Вместе с тем, могут наблюдаться такие ситуации, когда самостоятельное значение имеют и отдельные подгруппы среди более общей логически обособленной группы прав и полномочий. В этом случае создается группа логически связанных ролей, каждая из которых может выполняться только в совокупности с другими ролями данной группы. В этих ситуациях назначение подобной роли для пользователя может иметь смысл только тогда, когда он одновременно получает и другие роли из соответствующего логически связанного набора ролей. Для реализации подобного подхода на множестве ролей $\mathfrak{R}$ вводится функция $f^{\rho}_{\text{prerequisite}}: \mathfrak{R} \to \mathcal{R}$, определяющая для любой роли **ρ** набор **R** ∈ $\mathfrak{R}$ логически связанных с ней ролей, и устанавливается соответствующее ограничение на отношение **FU$\mathfrak{R}$**:
для $\forall (u, \rho) \in F_{U\mathfrak{R}}(u) \wedge \rho' \in f^{\rho}_{\text{prerequisite}}(\rho) \Rightarrow (u, \rho') \in F_{U\mathfrak{R}}(u)$.

В заключение рассмотрения разновидностей ролевых моделей в плане их критического анализа заметим, что помимо необходимости отмеченной ранее дополнительной регламентации отображения **FP$\mathfrak{R}$** при иерархической структуре

системы ролей, можно было бы по аналогии с тематико-иерархическим подходом ввести понятие мультиролей, и на этой основе более строго регламентировать назначение пользователям иерархически организованных ролей, а также механизмы взаимоисключающих ролей, количественных ограничений и группирования ролей.

В практическом применении могут использоваться комплексные подходы, сочетающие все рассмотренные разновидности ролевых моделей, что позволяет существенно упростить проектирование и администрирование систем разграничения доступа для КС, автоматизирующих сложные, нетривиальные организационно-технологические и организационно- управленческие схемы и процессы. Вместе с тем, в ролевых моделях нет строгих доказательств безопасности системы в соответствии с определенными формализованными критериями. Поэтому их безопасность основывается на контрольных механизмах дискреционных или мандатных моделей, средствами которых регулируется доступ ролевых субъектов к объектам системы.

2.4.3. Индивидуально-групповое разграничение доступа

Технологии рабочих групп пользователей, лежащие в основе систем индивидуально-группового разграничения доступа, представляют упрощенную, но наиболее широко применяемую разновидность ролевой политики разграничения доступа.

Основные положения модели индивидуально-группового разграничения доступа сводятся к следующему.

1. КС представляется совокупностью следующих наборов сущностей:

- множества объектов доступа **O (o1, o2,…, oM)**;
- множества пользователей **U (u1, u2,…, uN)**;
- множества рабочих групп пользователей **G (g1, g2,…, gK)**;
- множества прав доступа и привилегий **R (r1, r2,…, rJ)**;

- матрицей доступа **A** размерностью ((N +K) x M), каждая ячейка которой специфицирует права доступа и привилегии пользователей или их рабочих групп к объектам из конечного набора прав доступа и привилегий **R (r1, r2,…, rJ)**, т. е. **A[u, o] ⊆ R**, **A[g, o] ⊆ R**.

Определение 2.4.2. Рабочей группой называется совокупность пользователей КС, объединенных едиными правами доступа к объектам и (или) едиными привилегиями (полномочиями) выполнения определенных процедур обработки данных.

Нетрудно видеть, что рабочая группа представляет упрощенный аналог некоторой роли, которая формируется «снизу», т. е. на основе агрегирования в одну общую сущность пользователей, потребности в доступе которых к объектам системы подобны или близки. С учетом того, что полное совпадение потребностей пользователей в правах доступа к объектам системы в большинстве случаев маловероятно, у пользователей сохраняются и индивидуальные права доступа, которые не охватываются правами рабочей группы.

2. Групповые отношения в системе устанавливаются отображением множества пользователей на множество рабочих групп: **FUG: U x G** – такое, что одна рабочая группа объединяет нескольких пользователей, а один пользователь может входить в несколько рабочих групп.

Выражаясь языком моделей организации данных, можно отметить, что между сущностями «Рабочие группы» и сущностями «Пользователи» устанавливаются связи «Многие-ко-Многим». Данное обстоятельство обусловлено тем, что если рабочие группы рассматривать как агрегирование полномочий для выполнения пользователями определенных функциональных задач (обязанностей), то в реальных ситуациях один пользователь последовательно или на постоянной основе может выполнять сразу несколько задач (обязанностей), и ему тем самым необходимы права сразу нескольких рабочих групп. С другой стороны, сходные задачи

могут решаться сразу несколькими пользователями, и, отсюда, одна рабочая группа объединяет нескольких пользователей.

Заметим также, что отношение **FUG** обеспечивает второй этап организации ролевого разграничения доступа. При этом, однако, в отличие от классической ролевой политики, в технологии рабочих групп разделение процесса функционирования системы на сеансы не является принципиальным, ввиду того, что пользователь, входя в систему, всегда приобретает помимо своих индивидуальных прав одновременно и права доступа всех рабочих групп, в которые он включен по отношению **FUG.**

3. Функционирование системы индивидуально-группового разграничения доступа основывается на введении и использовании следующих функций:

fgroups: **U→ G** – значением функции **f**groups**(u) = G** является набор рабочих групп **G = {gu1, gu2 ,…} ⊆ G**, в которые пользователь **u** включен по отображению **FUG**;

fusers: **G → U** – значением функции **U = f**users**(g)** является набор пользователей **U = {ug1, ug2 ,…} ⊆ U**, которые рабочая группа **g** включает по отношению **FUG**.

В практическом плане реализация функций **f**groups и **f**users производится посредством построения бинарной матрицы «Пользователи-Рабочие Группы», ячейки которой заполняются при установлении отношения **FUG.**

4. Управление индивидуально-групповым доступом в системе осуществляется на основе следующего правила (критерия безопасности) индивидуально-группового доступа.

Правило 2.4.2. Система функционирует безопасно, если и только если любой пользователь **u ∈ U** по отношению к любому объекту **o ∈ O** может осуществлять доступ с правами **R**, не выходящими за пределы совокупности индивидуальных прав **A[u, o]** и прав рабочих групп $\mathbf{A}[\tilde{g}^{(u)}_i, o]$, в которые пользователь входит по отношению **FUG**:

R ⊆ {A[u, o] ∪ A[gu1 , o] ∪ A[gu2 , o] ∪…}, где **{ gu1 , gu2** ,…**} = f**groups**(u).**

Таким образом, права доступа пользователя к объекту складываются из его индивидуальных прав и прав всех рабочих групп, в которые он включен по отношению **FUG**.

При этом следует отметить, что рабочие группы в полном смысле слова не являются ролями, так как, хотя и представлены в матрице доступа отдельными строками, тем не менее, не реализуются в виде отдельных и самостоятельно действующих субъектов доступа КС. В практическом плане это означает, что в КС не инициализируются отдельные субъекты доступа (процессы, запущенные программы, приложения и т. п.), действующие от имени рабочих групп. Иначе говоря, в системе индивидуально- группового доступа действуют только субъекты пользователей, права которых в процессах доступа к объектам определяются на основе совокупности индивидуальных и групповых прав.

Заметим также, что в приведенной спецификации модели индивидуально-группового доступа, как и в других разновидностях ролевых моделей, нет доказательства безопасного функционирования системы при выполнении правил разграничения доступа. Поэтому нетрудно видеть, что в смысле механизмов безопасности модель индивидуально-группового доступа полностью идентична дискреционным моделям, основанным на матрице доступа.

Содержание и, если так можно выразиться, сила моделей индивидуально-группового доступа, определившие их чрезвычайно широкое распространение, в другом. Через агрегирование субъектов доступа (пользователей) в рабочие группы удается существенно упростить проектирование (синтез) и управление (анализ) системы дискреционного разграничения доступа в ситуациях с большим количеством пользователей и большим количеством объектов доступа, т. к. в дискреционных системах, на- помним, требуется отдельное и явное «прописывание» в матрице доступа (в списках доступа объектов) разрешений на доступ для любой пары

«субъект(пользователь)-объект» и по любому методу доступа (чтение, запись и т. д.). Поэтому предоставление пользователям прав доступа к объектам через рабочие группы позволяет существенно уменьшить количество индивидуальных назначений, упростить, упорядочить проектирование и анализ системы коллективного доступа к ресурсам КС.

Как и в классическом ролевом подходе, дополнительными аспектами организации системы разграничения доступа являются возможные отношения на множестве прав и отношения на множестве рабочих групп.

В рамках теоретико-множественной модели прав и привилегий (множество **R**) все конкретные права доступа и привилегии (элементы множества **R**) равнозначны и независимы. Однако в реальности это не всегда так. К примеру, право **Modify** «сильнее», т. е. охватывает права **Write** и **Read.** В большинстве случаев можно считать, что отношения «силы» (охватности) прав (методов) доступа рефлексивны, антисимметричны и транзитивны. В формальном плане это означает, что на множестве R устанавливается отношение частичного порядка: **FRR: R x R** - отношение, определяющее относительную силу (охватность) одних прав доступа по отношению к другим правам и задающее оператор доминирования $\geq$ такое, что если для **r1, r2** $\in$ **R, r1** $\geq$ **r2**, то право (метод доступа) **r1** сильнее, чем **r2**, т. е. охватывает, включает потоки информации, вызываемые методом доступа **r2.**

В результате простое объединение наборов прав дополняется следующим ограничением:

$$\forall\ \mathbf{r1, r2} \in \mathbf{R, r1} \geq \mathbf{r2} \wedge \mathbf{r2} \in \mathbf{R} \Rightarrow \mathbf{r2} \notin \mathbf{R},$$

где $\mathbf{R = \{A[u, o] \cup A[gu1, o] \cup A[gu2, o] \cup \ldots\}}$;

u и **o** – пользователь и объект доступа, соответственно;

{gu1 , gu2 ,…} = fgroups**(u)** – набор рабочих групп, в которые включен пользователь **u.**

Теоретико-множественное объединение индивидуальных и групповых прав доступа с учетом данного ограничения будем обозначать $\cup<$. Таким образом, итоговый

набор прав субъекта-пользователя в системе индивидуально-группового разграничения доступа по правилу 2.4.2 определяется следующим соотношением:

$$\mathcal{R} = \{\mathbf{A}[u, o] \cup^{<} \mathbf{A}[g_{u_1}, o] \cup^{<} \mathbf{A}[g_{u_2}, o] \cup^{<} \dots\}.$$

Существенным фактором при определении прав доступа, складывающихся по нескольким возможностям доступа (например, по индивидуальным и групповым назначениям; по прямым назначениям к объекту и по наследуемым правам доступа к объекту от контейнера), является обеспечение в определенных случаях гарантированного непредоставления (гарантированного запрета) определенному пользователю определенного права доступа к определенному объекту. Если права доступа определяются на основе одного варианта, скажем только на основе индивидуальных назначений без использования рабочих групп и иных агрегаций, то непредоставление прав доступа эквивалентно отсутствию разрешения на доступ.

В случае же индивидуально-группового доступа при отсутствии индивидуального права на доступ к объекту или права на доступ к объекту по какой-либо одной рабочей группе, пользователь может получить нежелательный доступ к данному объекту по другой рабочей группе. При этом такие ситуации могут быть вполне обоснованными, так как для всех остальных членов группы, по которой пользователь получает нежелательный доступ, данные права являются обоснованными и необходимыми, а исключить пользователя из данной группы также нельзя, так как он при этом может потерять набор других необходимых ему прав.

Разрешение данной проблемы осуществляется двумя способами:

- введением механизма ограниченного членства пользователя в группе;
- введением специфического права доступа, именуемого «запрет доступа».

Первый способ основывается на введении для каждого члена рабочей группы индивидуального «фильтра»

наследования групповых прав. При этом, однако, данный способ, предоставляя возможность гибкой настройки индивидуально-групповых прав доступа на различные организационно-технологические и управленческие схемы, тем не менее, для решения проблемы гарантированного непредоставления прав требует просмотра и анализа всех групповых назначений, в которые включен данный пользователь.

Для вводимого же права «запрет доступа» устанавливается самый высокий приоритет в отношении частичного порядка на множестве прав доступа **R**. В результате проблема гарантированного непредоставления права доступа решается автоматически. Если среди индивидуальных либо групповых назначений пользователя к объекту имеется явный запрет на доступ, то все остальные назначенные права отвергаются.

Во многих практических системах допускается включение одних рабочих групп в другие, иначе говоря, членами рабочих групп кроме пользователей могут быть и коллективные пользователи, т. е. другие рабочие группы.

Ясно, что с учетом сущности рабочих групп, как объединений пользователей, подобные отношения должны быть исключительно транзитивными. Иначе говоря, ситуации, когда группа A входит в группу B, группа входит в группу C, а группа C входит в группу A, недопустимы и бессмысленны. Ясно также, что отношения рабочих групп должны быть антисимметричны – если группа A входит в группу B, то группа B, в свою очередь, не может входить в группу A. Кроме того, смыслу группы как объединению пользователей не противоречит утверждение, что группа входит сама в себя, иначе говоря, отношения групп рефлексивны.

Отсюда следует, что на множестве рабочих групп G можно устанавливать отношение **FGG: G x G** - отношение частичного порядка, определяющее иерархию (вложенность) рабочих групп и задающее оператор доминирования $\geq$ такое, что если для $\mathbf{g1, g2} \in \mathbf{G}$, $\mathbf{g1} \geq \mathbf{g2}$, то **g1** включает **g2**.

Соответственно для управления доступом в системах с вхождением одних рабочих групп в другие требуется введение и использование дополнительной функции $f^{h}_{groups}: G \to G$ – значением функции **f**groups**(g)** является набор рабочих групп **{gg1, gg2 ,…}** ⊆ **G** , в которые рабочая группа **g** включена по отношению **FGG**.

В практическом плане реализация функции f^{h}_{groups} совместно с функциями **f**groups и **f**users может производиться на основе расширения бинарной матрицы «Пользователи-Группы» строками, соответствующими рабочим группам системы, т. е. построением матрицы «(Пользователи+Группы)-Группы».

Частичный порядок на множестве групп, если так можно выразиться, «слабее» частичного порядка на множестве иерархической системы ролей- должностей, так как одна рабочая группа может входить сразу в несколько рабочих групп, часть рабочих групп может не входить ни в какие другие группы и не включать в себя другие группы. Это означает, что системы с иерархически организованными ролями описываются графом в виде корневого дерева, а система рабочих групп графом произвольного вида, в том числе и с иерархически организованными фрагментами – см. рис. 2.23. Главной особенностью графа рабочих групп должно быть отсутствие циклов, порождаемых цепочками транзитивности.

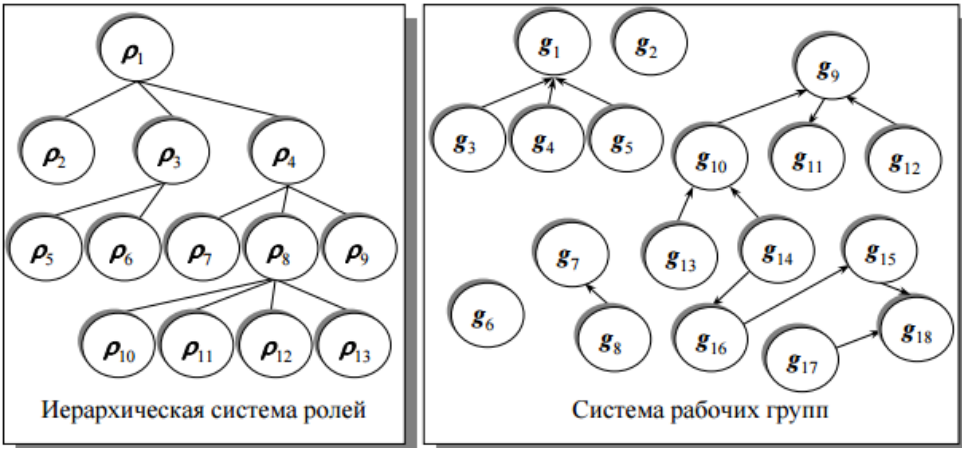

Рис. 2.23. Пример организации системы ролей и рабочих групп

В практических системах проблема транзитивности отношений в системе взаимосвязанных рабочих групп решается двумя способами:

• построением графа включения групп, поиском и исключением (разрывом) из него циклов;

• разделением множества групп на два подмножества – группы, которые могут входить в другие группы, но состоять только из пользователей, т. е. не могут содержать другие группы; и группы которые могут состоять как из пользователей, так и из групп, но сами входить в другие группы не могут.

Как правило, при втором способе группы первого вида не имеют своих собственных групповых прав и привилегий, а используются лишь для того, чтобы комплектовать рабочие группы второго вида «групповым» способом. Тем самым, обеспечивается структура, описываемая двудольным графом, все пути в котором имеют длину, равную единице, принципиально исключая на этой основе возможность транзитивных связей, порождающих циклы (см. рис. 2.24).

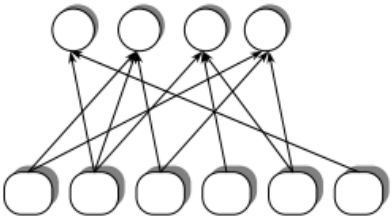

Рис. 2.24. Двудольная система рабочих групп

Из самого понятия рабочих групп как объединений сущностей однотипного доступа следует механизм наследования прав и полномочий «сверху», что также принципиально отличает технологию рабочих групп от ролевой модели. Данный механизм наследования можно выразить следующим правилом определения прав доступа и привилегий рабочих групп пользователей.

Правило 2.4.3. Полный набор прав и полномочия **Rg** рабочей группы пользователей **g** к объекту o определяются совокупностью набора прав и привилегий **A[g, o]**, непосредственно предоставленных данной группе, и набором прав и привилегий рабочих групп **A[ggi, o]**, в которые по отношению **FGG** может входить данная рабочая группа:

$$\mathcal{R}_g(o) \subseteq \{\mathbf{A}[g, o] \cup^{<} \mathbf{A}[g_{g_1}, o] \cup^{<} \mathbf{A}[g_{g_2}, o] \cup^{<} \dots\}, \text{где } \{g_{g_1}, g_{g_2}, \dots\} = f^{h}_{\text{groups}}(g).$$

Соответственно, критерий безопасности индивидуально-группового доступа необходимо скорректировать, включая в итоговый набор прав пользователя права и его рабочих групп:

$$\mathcal{R} \subseteq \{\mathbf{A}[u, o] \cup^{<} \mathcal{R}_{g_{u_1}}(o) \cup^{<} \mathcal{R}_{g_{u_2}}(o) \cup^{<} \dots\}.$$

В заключение отметим, что модель индивидуально-группового разграничения доступа обладает существенными выразительными возможностями при организации коллективного доступа к ресурсам в сложных системах с большим количеством пользователей и большим количеством сложно организованных и многочисленных ресурсов. Вместе с тем, ее использование помимо слабости защитных свойств

дискреционного принципа разграничения доступа, на котором она основывается, таит и некоторые другие «подводные» камни, такие как избыточность и дублирование в предоставлении прав доступа пользователей к объектам системы. Кроме того, в ряде случаев проектирование системы рабочих групп представляет нетривиальную задачу, и требует применения дополнительных теоретико-графовых алгоритмов и пространственно-векторных моделей.

3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАЛИЗУЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

3.1. Термины и определения

Определение 3.1.1. **Автоматизированная система:** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Определение 3.1.2. **Агент нарушителя:** лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

Определение 3.1.3. **Активы** (assets): все, что имеет ценность для организации и находится в ее распоряжении.

Определение 3.1.4. **Блокирование доступа (к информации):** прекращение или затруднение доступа законных пользователей к информации.

Определение 3.1.5. **Вредоносная программа:** программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Определение 3.1.6. **Глубина анализа скрытого канала:** степень варьирования применяемых средств по сложности для идентификации скрытого канала и его характеристик.

Определение 3.1.7. **Доверие** (assurance): основание для уверенности в том, что объект соответствует целям безопасности.

Определение 3.1.8. **Идентификация скрытого канала:** выявление возможности существования скрытого канала и определение его места в классификации.

Определение 3.1.9. **Информация ограниченного доступа:** вид сведений, доступ к которым ограничен и разглашение которых может нанести ущерб интересам других лиц, общества и государства.

Определение 3.1.10. **Информационная безопасность** (information security): все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Определение 3.1.11. **Информационная система:** организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Определение 3.1.12. **Информационная технология:** приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных использования данных.

Определение 3.1.13. **Информационный объект:** элемент программы, содержащий фрагменты информации, циркулирующей в программе.

Определение 3.1.14. **Информационный поток** (information flow): процесс взаимодействия источника информации и ее получателя.

Определение 3.1.15. **Исчерпывающий анализ скрытых каналов** (exhaustive covert channel analysis): анализ,

при котором требуется представление дополнительного свидетельства, показывающего, что план идентификации скрытых каналов достаточен для утверждения того, что были испробованы все возможные пути исследования скрытых каналов.

Определение 3.1.16. **Ключ:** конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Определение 3.1.17. **Коммуникационный канал:** совокупность носителей информации, доставляющих сообщение от источника к приемнику.

Определение 3.1.18. **Критически важные объекты:** объекты, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени.

Определение 3.1.19. **Механизм передачи информации:** реализованный способ передачи информации от отправителя к получателю.

Определение 3.1.20. **Модификация информации:** целенаправленное изменение формы представления и содержания информации.

Определение 3.1.21. **Нарушитель безопасности информации** (adversary): физическое лицо (субъект), случайно

или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Определение 3.1.22. **Несанкционированный доступ к информации** (unauthorized access to information): доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Определение 3.1.23. **Объект** (object): пассивный компонент системы, хранящий, принимающий или передающий информацию.

Определение 3.1.24. **Оценка опасности:** определение степени возможного деструктивного воздействия.

Определение 3.1.25. **Оценочный уровень доверия** (evaluation assurance level): пакет компонентов доверия, представляющий некоторое положение на предопределенной в нем шкале доверия.

Определение 3.1.26. **Пароль доступа** (password): идентификатор субъекта доступа, который является его (субъекта) секретом.

Определение 3.1.27. **Персональные данные:** любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Определение 3.1.28. **Политика безопасности информации** (information security policy): совокупность документированных правил, процедур, практических приемов

или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Определение 3.1.29. **Продукт** (product): совокупность программных, программно-аппаратных и/или аппаратных средств информационных технологий, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

Определение 3.1.30. **Пропускная способность скрытого канала**
(covert channel capacity): количество информации, которое может быть передано по скрытому каналу в единицу времени или относительно какой-либо другой шкалы измерения.

Определение 3.1.31. **Система** (system): специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

Определение 3.1.32. **Систематический анализ скрытых каналов** (systematic covert channel analysis): анализ, при котором разработчик системы информационных технологий и автоматизированных систем должен идентифицировать скрытые каналы структурированным и повторяемым образом в противоположность идентификации скрытых каналов частным методом, применимым для конкретной ситуации.

Определение 3.1.33. **Скрытый канал** (covert channel): непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Определение 3.1.34. **Среда передачи**: физическая реализация процесса передачи информации.

Определение 3.1.35. **Субъект** (subject): активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, которые могут явиться причинами потока информации от объекта к объекту или изменения состояния системы.

Определение 3.1.36. **Угроза безопасности** (threat): совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Определение 3.1.37. **Уполномоченный пользователь** (authorised user): пользователь, которому в соответствии с политикой безопасности разрешено выполнять какую-либо операцию.

Определение 3.1.38. **Ущерб:** отрицательные последствия, возникающие вследствие причинения вреда активам.

Определение 3.1.39. **Уязвимость:** свойство системы, которое можно использовать для нарушения информационной безопасности системы информационных технологий и автоматизированных систем.

3.1.2. Общие сведения о скрытых каналах

Развитие, внедрение и использование распределенных информационных систем и технологий, использование импортных программно-аппаратных платформ без конструкторской документации привели к появлению класса угроз информационной безопасности (ИБ), связанных с

использованием так называемых скрытых информационных каналов, «невидимых» для традиционных средств защиты информации.

Традиционные средства обеспечения ИБ такие, как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только информационные потоки, которые проходят по каналам, предназначенным для их передачи. Возможность обмена информацией вне этих рамок посредством скрытых каналов (СК) не учитывается.

В системах, требующих обеспечения повышенного уровня доверия, должны учитываться угрозы безопасности, возникающие вследствие наличия возможности несанкционированного действия с помощью СК.

Опасность СК для информационных технологий (ИТ) и автоматизированных систем (АС) и других активов организации связана с отсутствием контроля средствами защиты информационных потоков, что может привести к утечке информации, нарушить целостность информационных ресурсов и программного обеспечения в компьютерных системах или создать иные препятствия по реализации ИТ.

Для обеспечения защиты информации, обрабатываемой в АС, необходимо выявлять и нейтрализовывать все возможные информационные каналы несанкционированного действия - как традиционные, так и скрытые.

Настоящий стандарт входит в серию взаимосвязанных стандартов, объединенных общим наименованием «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов», включающий в себя:

- общие положения;
- рекомендации по организации защиты информации, ИТ и АС от атак с использованием СК.

В общих положениях определены задачи, решаемые при проведении анализа СК, описана классификация СК и

приведена классификация активов по степени опасности атак с использованием СК.

Существенным моментом защищенности систем ИТ и АС является доверие к системам защиты. Обеспечение доверия осуществляется путем глубокого анализа или экспертизы программно-аппаратных продуктов с точки зрения их защищенности. Во многих случаях этот анализ затруднен в силу отсутствия исходных данных для его проведения, то есть исходных кодов, конструкторской и тестовой документации, в результате чего создаются угрозы информационным ресурсам, которые могут быть реализованы с помощью неизвестных программно-аппаратных систем и через интерфейсы взаимодействующих программно-аппаратных продуктов.

Требования доверия к безопасности информации установлены в ГОСТ Р ИСО/МЭК 15408-3, в соответствии с которым для систем с оценочным уровнем доверия (ОУД), начиная с ОУД5, предусмотрено проведение обязательного анализа СК. При использовании аппаратно-программных продуктов иностранных производителей в условиях отсутствия на них конструкторской, тестовой документации и исходных кодов невозможно гарантировать отсутствие в них потенциально вредоносных компонентов, включенных специально или возникших случайно (например, программной уязвимости). Таким образом, требование анализа СК в Российской Федерации является необходимым условием безопасного функционирования систем, обрабатывающих ценную информацию или использующих импортное аппаратно-программное обеспечение, в том числе и для систем с ОУД ниже ОУД5.

В рекомендациях по организации защиты информации, ИТ и АС от атак с использованием СК определен порядок поиска СК и противодействия СК.

Настоящий стандарт разработан в развитие ГОСТ Р ИСО/МЭК 15408-3, ГОСТ Р ИСО/МЭК 17799 (в части мероприятий по противодействию угрозам ИБ, реализуемым с использованием СК).

Классификация защищаемых активов в зависимости от степени опасности атак с использованием СК.

Глубину анализа СК определяют ценностью активов, то есть ущербом, который может быть причинен в результате реализации угроз безопасности, реализуемых с использованием СК, то есть рисков, возникающих вследствие наличия этих угроз.

Идентификация СК определяет субъекты (источник и получателя), между которыми потенциально может существовать СК, параметры, при манипулировании которыми происходит передача информации, параметры, за счет вариации которых происходит чтение информации, среду передачи информации, логические условия, при которых возможна передача информации. Идентификация СК может проводиться как при разработке системы путем исследования потенциальных каналов утечки или каналов воздействия, так и в режиме эксплуатации системы путем наблюдения признаков, идентифицирующих наличие СК. В последнем случае СК выявляются с помощью наблюдения за параметрами системы. В документации по безопасности информации должно быть отражено, какие классы СК могут быть выявлены с помощью используемой системы наблюдения.

Оценку пропускной способности идентифицированных СК проводят формальными, техническими методами или методами моделирования.

При принятии решений о внедрении защитных мер для противодействия угрозам безопасности, реализуемым с использованием СК, необходимо учитывать возможный риск нанесения ущерба активам организации, который связан в том числе с пропускной способностью СК.

Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

- построение архитектуры ИТ или АС, позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными. Этот метод применяется на этапе проектирования ИТ или АС;

- использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность ниже заданного уровня;

- использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы. Выявление признаков работы СК может позволить блокировать их воздействие на информационные ресурсы;

- применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

3.1.3. Классификация скрытых каналов

СК по механизму передачи информации подразделяют на:

- СК по памяти;
- СК по времени;
- скрытые статистические каналы.

СК по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий - считывает ее.

Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация.

СК по памяти предполагают использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты.

СК по времени предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени. Например, в многозадачной операционной системе (ОС) центральный процессор является

разделяемым информационно-вычислительным ресурсом для прикладных программ. Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные.

Скрытый статистический канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями.

Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре СК.

Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

СК по памяти, в свою очередь, подразделяют на:

- СК, основанные на сокрытии информации в структурированных данных;
- СК, основанные на сокрытии информации в неструктурированных данных.

СК, основанные на сокрытии информации в структурированных данных, используют встраивание данных в информационные объекты с формально описанной структурой и формальными правилами обработки. Например, внутренний формат файлов, используемых современными текстовыми процессами, содержит ряд полей, не отображаемых при редактировании файла, поэтому они могут быть использованы для вставки скрытой информации. СК, основанные на сокрытии информации в неструктурированных данных, используют встраивание данных в информационные объекты без учета формально описанной структуры (например, запись

скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения).

СК по пропускной способности подразделяют на:

- канал с низкой пропускной способностью;
- канал с высокой пропускной способностью.

СК является каналом с низкой пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

СК является каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого данные информационные объекты являются ценными.

Для решения сложных задач может использоваться комбинация СК, опирающихся на различные механизмы передачи.

3.1.4. Классификация угроз безопасности, реализуемых с использованием скрытых каналов

Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Реализация данных угроз может привести к:

- нарушению конфиденциальности информационных активов;
- нарушению работоспособности ИТ и АС;
- блокированию доступа к ресурсам4;
- нарушению целостности данных и ПО.

Системами, наиболее подверженным атакам с использованием СК, являются:

- многопользовательские распределенные системы;
- системы с выходом в глобальные сети;
- системы, использующие криптографические средства защиты;
- системы, использующие многоуровневую (мандатную) политику разграничения доступа;
- системы, программно-аппаратные агенты в которых не могут быть обнаружены (в связи с использованием программного и аппаратного обеспечения с недоступным исходным кодом и в связи с отсутствием конструкторской документации).

Взаимосвязь угроз, реализуемых с помощью СК, с типами СК в зависимости от их пропускной способности приведена в таблице ниже.

Взаимосвязь угроз, реализуемых с помощью скрытых каналов, с типами скрытых каналов в зависимости от их пропускной способности

Угроза	Тип скрытых каналов	
	Скрытые каналы с низкой пропускной способностью	Скрытые каналы с высокой пропускной способностью
Внедрение вредоносных программ и данных	+	+
Подача злоумышленником команд агенту для выполнения	+	+
Утечка криптографических ключей или паролей	+	+
Утечка отдельных информационных объектов	-	+
Примечание - знак "+" - означает, что имеется связь угрозы с соответствующим типом скрытого канала; знак "-" - означает, что связи не существует.		

3.1.5. Классификация активов по степени опасности атак с использованием скрытых каналов

В зависимости от степени опасности атак с использованием СК защищаемые активы организации подразделяют на следующие классы:

1-й класс - активы, содержащие информацию, степень подверженности которой атакам, реализуемым с использованием СК, определяет собственник.

2-й класс - активы, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам.

3-й класс - активы, содержащие сведения, составляющие государственную тайну.

Кроме того, существует особый класс активов, которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью. К этой группе относятся:

Класс А - активы, связанные с функционированием критически важных объектов. Например, передача команды, способной инициализировать деструктивное воздействие на объект такого типа, может быть осуществлена по СК с низкой пропускной способностью.

Класс Б - активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам. Например, утечка ключевой/парольной информации по СК может поставить под угрозу функционирование всей информационной системы.

3.1.6. Механизм функционирования скрытого канала

СК используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на АС, которая не обнаруживается средствами контроля и защиты.

Опасность СК основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации.

Общая схема механизма функционирования СК в АС представлена на рис. 3.1.

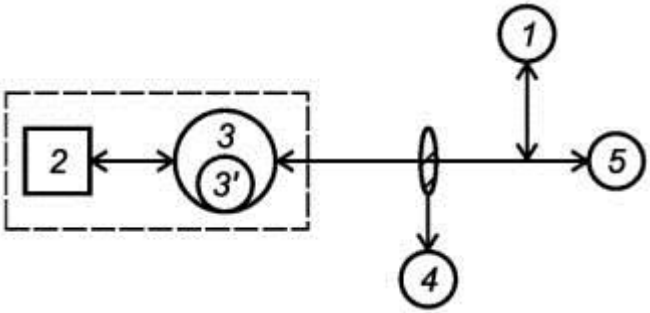

Рис. 3.1. Общая схема механизма функционирования СК в АС

На рис. 3.1: 1 - нарушитель безопасности (злоумышленник), целью которого является НСД к информации ограниченного доступа либо несанкционированное влияние на АС;

2 - информация ограниченного доступа либо критически важная функция;

3 - субъект, имеющий санкционированный доступ к 2 и 5;

3 - агент нарушителя безопасности, находящийся в замкнутом контуре с 2 и взаимодействующий с 2 от имени субъекта 3;

4 - инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий(ее) информационное взаимодействие 3, пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды;

5 - субъект, находящийся вне замкнутого контура, с которым 3 осуществляет санкционированное информационное взаимодействие.

Взаимодействие между субъектами 3 и 5 является санкционированным и необходимым для правильной работы АС. Задача агента 3 заключается в том, чтобы обеспечить регулярное интерактивное взаимодействие между агентом и злоумышленником. Агент должен передать информацию ограниченного доступа 2 злоумышленнику 1 либо по команде злоумышленника 1 оказать воздействие на критически важную функцию 2. Скрытность канала взаимодействия между злоумышленником 1 и агентом 3 заключается в том, что субъект 3, инспектор 4 и субъект 5 не обнаруживают факт передачи информации или команды.

СК позволяют злоумышленнику регулярно интерактивно осуществлять взаимодействие со своим агентом, внедренным в АС.

В АС взаимодействие между агентом 3 и субъектом 5 может быть, как сетевым, так и происходить внутри одной АС.

Классификация СК по различным признакам приведена в ГОСТ Р 53113.1.

Примеры СК, поясняющие механизм их функционирования, представлены ниже.

Пример 1 - Нарушитель безопасности (злоумышленник), сотрудничающий с конкурирующей организацией, в процессе внедрения (ввода в эксплуатацию) установил в АБС программного агента. Взаимодействуя с АБС в качестве клиента этого банка, злоумышленник передает программному агенту команды, закодированные в последовательностях его действий, каждое из которых не вызывает подозрений (проверка состояния счета, управление счетом, временные интервалы между операциями и др.). В ответ на команды,

полученные по СК, агент по тем же СК возвращает злоумышленнику интересующие конкурента сведения об атакуемом банке (информацию о счетах других клиентов, объемах активов банков, любую другую инсайдерскую информацию, к которой агент имеет доступ) либо вносит изменения в базу данных о счетах клиентов или любую другую информацию, к которой он имеет доступ. Выявление существования такого агента может произойти только по косвенным признакам, которые могут возникнуть в результате появления изменений в базах данных. Скрытая утечка информации из базы данных, происходящая по такому СК, будет оставаться незамеченной. В этом случае в соответствии со схемой на рисунке 1:3 - программный агент, 3 - АБС, 2 - база данных, 4 - служба безопасности банка, 1 - злоумышленник, действующий в интересах конкурента, 5 - клиент банка.

Пример 2 - Злоумышленник, имеющий целью получение служебной информации с компьютера сотрудника, может действовать по следующему сценарию. Пусть ПК, защищенный межсетевым экраном, заражен троянской программой. Троянская программа получает от злоумышленника команды и отправляет в ответ на них информацию о зараженном ПК и хранящуюся на нем информацию ограниченного доступа, маскируя обмен как протокол HTTP, разрешенный межсетевым экраном. В этом случае в соответствии со схемой на рис. 3.1: 1-3-троянская программа, 3 - программа, имеющая санкционированный доступ в Интернет, 2 - документ ограниченного распространения, 4 - межсетевой экран, 5 - узел сети Интернет, 1 - промежуточный узел сети, контролируемый злоумышленником.

3.1.7. Правила формирования модели угроз безопасности с учетом существования скрытых каналов

Модель угроз безопасности формируется с учетом угроз, реализуемых с использованием СК. Эти угрозы должны учитываться при оценке рисков ИБ.

Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Угроза внедрения вредоносных программ и данных заключается в том, что, обладая возможностью интерактивно взаимодействовать с атакуемой АС, злоумышленник может передать в нее посредством СК вредоносные программы, обладающие необходимой ему функциональностью. Внедрение ложных данных в атакуемую АС может осуществлять непосредственно агент, с которым злоумышленник взаимодействует по СК. Например, если агент внедрен в СУБД банка, злоумышленник может передать ему команду на изменение хранящихся в базе данных сведений о счетах клиентов либо подменить хранящуюся в этой базе процедуру, оперирующую с данными о счетах, ложной, вредоносной процедурой, действующей в интересах злоумышленника.

Угроза подачи злоумышленником команд агенту для выполнения его функций заключается в том, что агент может оказывать влияние на АС, в которую он внедрен, по команде злоумышленника. Эти команды могут быть как простыми (например, заблокировать работу АС на некоторое время), так и более сложными (например, передать злоумышленнику по СК содержимое файла, хранящегося в атакуемой системе).

Угроза утечки криптографических ключей или паролей, отдельных информационных объектов возникает, если злоумышленнику удалось внедрить своего агента в АС так,

чтобы агент имел доступ к ценным информационным активам (например, криптографическим ключам, паролям), СК могут быть использованы для несанкционированной передачи такой информации злоумышленнику. Поскольку ключи имеют сравнительно небольшой объем, даже канал с низкой пропускной способностью способен обеспечить их утечку.

3.1.8. Анализ рисков и правила организации защиты информации

Выбор мер противодействия угрозам ИБ, реализуемым с использованием СК, должен основываться на технико-экономической оценке или других методах оценки ценности информации. Кроме того, должны учитываться такие последствия, как утрата доверия к организации или подрыв деловой репутации организации и ее руководителя.

Следует выявить, какие из защищаемых информационных активов могут быть интересны потенциальному злоумышленнику, обладающему возможностью:

- встроить своего агента в АС в процессе ее разработки, развертывания, внедрения или эксплуатации;
- обнаружить в АС уязвимость (или встроенного агента), которая может быть использована для организации СК и получения доступа к защищаемым активам.

Для анализа рисков можно применять методологию по ГОСТ Р 51901.

С целью снижения информационных рисков до приемлемого уровня должны быть выбраны и внедрены мероприятия по организации ЗИ от атак с использованием СК.

ЗИ, ИТ и АС от атак, реализуемых с использованием СК, является циклическим процессом, включающим в себя следующие этапы, повторяющиеся на каждой из итераций процесса:

- анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием СК;

- выявление СК и оценка их опасности для активов организации;

- реализация защитных мер по противодействию СК;

- организация контроля за противодействием СК.

Цикличность процесса защиты от угроз ИБ, реализуемых с использованием СК, определяется появлением новых способов построения СК, неизвестных на момент предыдущих итераций.

3.1.9. Рекомендации по порядку выявления скрытых каналов, методам реализации защитных мероприятий и организации контроля

Порядок выявления СК включает в себя:

- оценку архитектуры АС и имеющихся в ней коммуникационных каналов;

- выявление возможных путей обмена скрытой информацией между злоумышленником и его предполагаемым агентом в АС;

- оценку опасности выявленных СК для защищаемых активов организации;

- принятие решения о целесообразности противодействия каждому из выявленных СК.

Оценка архитектуры АС подразумевает выявление всех имеющихся в ней коммуникационных каналов и анализ взаимодействия ее компонентов на предмет потенциального использования их для организации СК. В результате проведения такого анализа должны быть выявлены компоненты АС, в которых потенциально могут быть использованы СК.

Выявление возможных путей обмена скрытой информацией между злоумышленником и его предполагаемым

агентом в АС проводится на основании общей схемы механизма функционирования СК (см. раздел 6). Следует для каждого из защищаемых активов 2 (см. схему на рис. 3.1) выявить, какие субъекты 3 имеют к ним доступ и при этом изолированы от внешней среды, но имеют возможность взаимодействовать с отдельными субъектами из внешней среды 5. При этом взаимодействие контролируется 4 и может также наблюдаться потенциальным злоумышленником 1. При наличии этих элементов должен рассматриваться вопрос о возможном наличии потенциального СК между агентом 3, встроенным в 3, и субъектами во внешней среде 1 или 5. В качестве примера такого СК может рассматриваться возможность злоумышленника наблюдать интервалы времени, формируемые компонентом АС, потенциально содержащим агента злоумышленника 1.

С точки зрения злоумышленника использовать СК для нарушения ИБ в тех сегментах АС, где он может обмениваться информацией со своим агентом, используя канал, не контролируемый средствами ЗИ, является нецелесообразным. В этом случае нет необходимости в скрытии факта обмена информацией, потому что такой обмен защитными средствами не контролируется.

При оценке возможности взаимодействия посредством СК следует учитывать «непрозрачность» для определенных типов СК отдельных сегментов АС.

После выявления СК следует оценить, насколько они реализуемы и опасны для защищаемых активов организации. Эта оценка определяется объемом активов, пропускной способностью СК и временным интервалом, в течение которого активы сохраняют ценность. На основании этой оценки каналы, не представляющие реальной опасности для активов, признаются неопасными.

На основании оценки опасности СК с учетом результатов проведенного анализа рисков делается вывод о целесообразности или нецелесообразности противодействия таким каналам.

В качестве примера на рис. 3.2 представлена семиуровневая модель взаимодействия открытых систем, определенная в подпункте 6.1.5 ГОСТ Р ИСО/МЭК 7498-1.

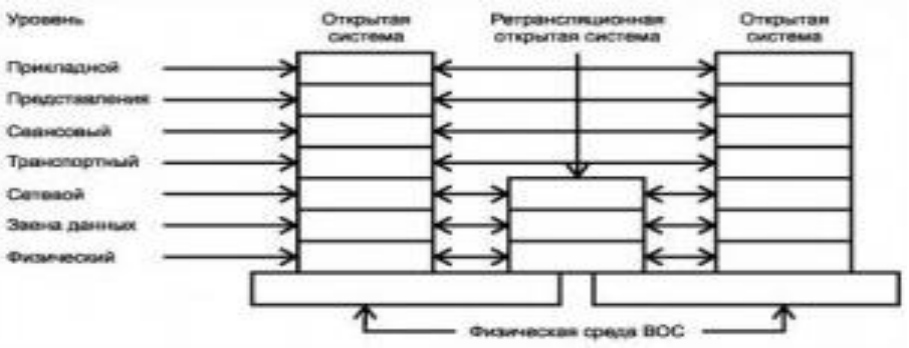

Рис. 3.2. Обмен данными через ретрансляционную открытую систему

Каждый из уровней данной модели взаимодействует только с нижестоящим и вышестоящим уровнями, при этом верхние уровни открытой системы изолированы от нижних. Эта особенность может быть использована для маскировки СК, действующих на низком уровне, от контролера, находящегося на высоком уровне.

В случае если специальные средства обнаружения СК не применяются, наличие СК может обнаружить пользователь какой-либо из взаимодействующих систем, наблюдая изменение поведения этих систем или частичную потерю их работоспособности.

Ограничивающим фактором при выборе злоумышленником уровня модели взаимодействия открытых систем в качестве среды для организации скрытой передачи является «непрозрачность» ретранслирующих систем. Ретранслирующие системы не содержат исходного отправителя и конечного получателя данных, а лишь передают данные от одних систем другим, если они не соединены единой физической средой в соответствии с ГОСТ Р ИСО/МЭК 7498-1.

При осуществлении ретрансляции в такой системе проводят интерпретацию полученной информации на всех уровнях модели, начиная с нижнего (физического) уровня, до уровня, на котором осуществляется ретрансляция данных. Затем, для передачи данных далее по сети, они вновь «спускаются» до физического уровня сети-получателя. В результате этого процесса, СК по памяти (см. п.п. 5.2 ГОСТ Р 53113.1), использующие особенности протоколов, относящихся к более низким уровням, чем тот, на котором осуществляется ретрансляция, могут уничтожаться или ограничивать возможности скрытой передачи информации сквозь такую ретранслирующую систему.

По результатам выявления СК формируется план мероприятий по противодействию угрозам, реализуемым с их использованием. Данные мероприятия могут включать в себя реализацию одного из уже известных (либо усовершенствование уже существующих) методов противодействия угрозам ИБ, реализуемым с использованием СК.

В качестве защитных мероприятий целесообразно использовать:

- снижение пропускной способности канала передачи информации;
- архитектурные решения построения АС;
- мониторинг эффективности защиты АС.

Выбор методов противодействия угрозам ИБ, реализуемым с использованием СК и формирование плана по их реализации, определяется экспертами, исходя из индивидуальных особенностей защищаемой АС.

Контроль за противодействием СК заключается в выявлении фактов использования СК в защищаемой АС. Такое выявление может проводиться непрерывно либо по факту обнаружения признаков ущерба от использования СК. Для выявления использования СК могут применяться статистический или сигнатурный методы.

Статистический метод выявления СК подразумевает сбор статистических данных о пакетах, проходящих через защищаемый участок сети, без внесения в них каких-либо изменений. Выявление СК может проводиться как в режиме реального времени (что позволяет быстро реагировать на инциденты), так и автономно, используя данные, накопленные за предыдущие отрезки времени, что делает возможным проведение более глубокого их анализа.

Метод выявления СК на основе сигнатурного анализа аналогичен способу, используемому антивирусными программами для поиска вредоносных программ. При наличии набора известных реализаций СК, для каждой из них формируется сигнатура, представляющая собой набор признаков, которые свидетельствуют о том, что используется данная реализация СК. Затем инспектор *4* (см. рисунок 1) проводит поиск таких сигнатур в просматриваемом потоке данных в сети и делает вывод о наличии или отсутствии в нем действующего СК в той или иной реализации. Для эффективной работы такого метода необходимо постоянное обновление базы сигнатур, т.е. включение в нее сигнатур для ранее неизвестных реализаций СК.

При выявлении признаков (в том числе косвенных) использования СК или появлении новых способов построения СК анализ рисков проводят повторно.

ЗАКЛЮЧЕНИЕ

В заключении рассмотрения основ моделирования безопасности компьютерных систем необходимо отметить, что на сегодняшний день это одна из наиболее развивающихся областей совместного практического применения математической теории и теории защиты информации. Постоянно появляются новые перспективные направления исследований, а уже имеющиеся получают еще более глубокую научную проработку.

К числу возможных перспективных направлений можно отнести:

- формализацию положений теории компьютерной безопасности;
- разработку моделей безопасности, более точно отражающих существующий уровень развития компьютерной техники и информационных технологий и более удобных для практического использования и анализа защищенности реальных систем, в ом числе информационных систем персональных данных, государственных информационных систем и автоматизированных систем управления критически важными объектами;
- разработка средств и методов противодействия угрозам информационной войны;
- вопросы обеспечения безопасности в глобальных информационных сетях;
- безопасность систем электронной коммерции.
- вопросы безопасности обработки информации мобильными пользователями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Башарин, Г. П. Модели информационно-вычислительных систем [Текст]: сб. науч. тр. / Г. П. Башарин. – М.: Наука, 1994. – 78 с.

2. Гайдамакин, Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. – Екатеринбург: изд-во Уральского университета, 2003. – 328 с.

3. Гайдамакин, Н. А. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие / Н. А. Гайдамакин. – Екатеринбург: изд-во Уральского университета, 2008. – 212 с.

4. Гайдамакин, Н. А. Автоматизированные информационный системы, базы и банки данных [Текст] / Н. А. Гайдамакин. – М.: Гелиос АРВ, 2002.

5. Галатенко, В. А. Основы информационной безопасности [Текст]: учеб. пособие / В. А. Галатенко; под ред. В. Б. Бетелина. – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.

6. Девянин, П. Н., Модели безопасности компьютерных систем [Текст]: учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

7. Грушо, А. А. Теоретические основы защиты информации [Текст] / А. А. Грушо, Е. Е. Тимонина. – М.: Яхтсмен, 1996. – 192 с.

8. Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах [Текст]: учеб. пособие для вузов / П. Н. Девянин. – М.: Радио и связь, 2006. – 176 с.

9. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. – М.: Радио и связь, 2000. – 192 с.

10. Девянин, П. Н. Модели безопасности компьютерных систем [Текст]: учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

11. Многофункциональные межсетевые экраны: методология разработки и технология применения [Текст] / В. С. Заборовский, А.П. Лубанец, С. В. Купреенко, А. В. Силиненко // Региональная информатика 2004 (РИ-2004): IX Санкт-Петербургская междунар. конф. – 2004. – С. 126.

12. Зегжда, Д. П. Основы безопасности информационных систем [Текст] / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия Телеком, 2000. – 452 с.

13. Корт, С. С., Теоретические основы защиты информации [Текст]: учеб. пособие / С. С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.

14. Мафтик, С. Механизмы защиты в сетях ЭВМ [Текст]: пер. с англ. / С. Мафтик. – М.: Мир, 1993. – 216с.

15. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] / В. В. Платонов. – М.: Академия, 2006. – 240 с.

17. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учеб. пособие / В. Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.

СОДЕРЖАНИЕ

Учебное издание

Куликов Сергей Сергеевич

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

В авторской редакции

Подписано к изданию 27.08.2015.

Объем данных 2,71 Мб.

ФГБОУ ВПО «Воронежский государственный технический университет»
394026 Воронеж, Московский просп., 14