

ДОСТАТОЧНЫЕ УСЛОВИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ СИСТЕМАХ

В.А. ГОРБАЧЕВ

Рассматриваются субъектно-объектная модель доступа, аксиоматические достаточные условия защищенности информации, а также требования, предъявляемые к мониторам безопасности в электронных системах.

Ключевые слова: политика безопасности, модель доступа, разграничения доступа, монитор безопасности, электронная система.

ВВЕДЕНИЕ

В настоящее время перед отечественными разработчиками сложных электронных систем (ЭС) стоят две противоречивые задачи:

1) реализовать довольно высокие требования безопасности к обработке информации;

2) сохранить в полном объеме совместимость с используемыми зарубежными электронными компонентами.

Основное противоречие состоит в том, что требование совместимости с зарубежными компонентами подразумевает их использование в составе защищенной системы. В то же время разработчики этих компонентов не ставили перед собой такой задачи в силу ориентации этих продуктов на массовый рынок. Поэтому встраивать дополнительные средства защиты в системы обработки информации специального назначения – занятие безнадежное, особенно в условиях отсутствия подробной технической документации и поддержки со стороны разработчиков этих компонентов. Таким образом, решение проблемы построения защищенных ЭС на базе таких компонентов является более чем актуальной задачей, причем ее решение требует развития новых подходов к проблеме проектирования защищенных ЭС.

Перед разработчиками современных электронных систем, предназначенных для обработки важной информации, стоят следующие задачи, требующие эффективного решения:

1) технологии проектирования должны основываться на принципах доказательно обеспечивающих гарантии защищенности систем;

2) интеграция средств защиты информации в процесс ее обработки в качестве обязательного элемента;

3) включение в механизмы защиты функций, обеспечивающих безопасность электронной системы в условиях возможного появления внутри ее компонентов, осуществляющих деструктивные действия.

Теоретические исследования, касающиеся моделей политики безопасности, ориентированы на программные системы [2, 3, 5] и не преследуют цель анализа безопасности информации в ЭС.

Целью данного исследования являются технологии проектирования защищенных ЭС, обеспечивающих устойчивость к деструктивному воздействию внутренних компонентов.

1. СУБЪЕКТНО-ОБЪЕКТНАЯ МОДЕЛЬ ЭС

Рассмотрим основные понятия субъектно-объектной модели ЭС. В ЭС действует дискретное время t . В каждый фиксированный момент времени t ЭС представляет собой конечное множество компонентов, разделяемых на два подмножества: субъектов доступа S ; объектов доступа O .

Определим эти абстрактные понятия и поставим им в соответствие физические представления в ЭС.

Объект (O) – часть ресурсов системы, находящаяся в момент времени t в пассивном состоянии относительно информации, а также других компонентов этой системы. Объект может быть источником нового субъекта, через процессы, которые локализованы в субъектах.

Субъект (S) – это компонент системы, находящийся в момент времени t в активном состоянии, который может изменять состояние системы с помощью субъектов. Субъекты могут породить новые объекты и субъекты в системе.

Будем считать, что все компоненты ЭС в различные моменты времени t_k могут представлять собой либо субъекты, либо объекты. Кроме того, предполагается, что в любой момент времени t , в том числе и в начальный, множество субъектов доступа S не пусто.

Источник угроз электронной системы, в дальнейшем **источник угроз (ИУ)**. В пассивном состоянии это совокупность объектов, в активном состоянии это субъект и связанные с ним объекты.

Рассматривая ИУ, как некоторый тип субъекта, который способен осуществить несанкционированный доступ, отметим следующие его особенности.

Во-первых, ИУ, являясь аппаратным, программно-аппаратным ресурсом ЭС, в пассивном состоянии может быть частью некоторого объекта.

Во-вторых, угрозы информации в ЭС могут исходить только от активного субъекта – ИУ, ко-

торый в текущий момент времени владеет функцией управления ресурсами.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты. Одним из результатов воздействия субъекта на объект могут быть порожденные в ЭС другие субъекты или состояния системы. Как частный случай – это активизация ИУ.

Можно выделить три компонента, связанные с процессом нарушения безопасности систем ИУ [4]:

ИУ – совокупность субъектов и объектов, представляющих нарушителя;

Объект атаки – часть системы, на которую ИУ производит воздействие;

Канал воздействия – физическая среда переноса злоумышленного воздействия.

Под **пользователем** будем понимать один или некоторую совокупность субъектов (S_0), действующих от имени пользователя [3, 5]. Пользователь ЭС, является, таким образом, внешним фактором, управляющим состоянием субъектов. Предполагается, что пользователь не может изменить свойства субъектов доступа. В общем, случае это условие не соответствует реальным системам, в том числе и ЭС, в которых пользователи могут изменять свойства субъектов через изменение программ, программируемых устройств и т.д. Подобная идеализация позволяет построить четкую схему процессов и механизмов доступа, а угрозы безопасности, возникающие вследствие подобных реалий, рассматривать в контексте гарантий выполнения политики разграничения доступа через механизмы неизменности свойств ЭС.

Определим понятие **нарушителя**. В отличие от пользователя, действия нарушителя направлены на нарушение безопасности информации через несанкционированную возможность менять свойства отдельных субъектов и объектов, например, программируемых устройств или активизировать ИУ с помощью субъектов S_0 . Включение такого субъекта в состав системы приводит к тому, что условие неизменности свойства субъектов доступа нарушается. Очевидно, что нарушитель является частным случаем пользователя.

2. МОДЕЛЬ ДОСТУПА В ЭЛЕКТРОННЫХ СИСТЕМАХ

Рассмотрим понятие доступа в ЭС. Понятие доступа является одним из основополагающих в теории защиты информации.

Исходя из этого, центральным положением субъектно-объектной модели является следующее: все процессы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации [2, 3]. Практически, безопасность системы обеспечивается разрешением или запретом доступа для заданных множеств субъектов и объектов. В работе ин-

терпретация понятия доступа в ЭС имеет свои специфические особенности.

В общем случае, механизм доступа (в том числе и несанкционированного), реализуемый субъектом, может быть представлен как выполнение этим субъектом определенных действий над объектом с целью порождения нового субъекта или осуществления обмена информацией между объектами.

Для формализации механизма доступа в субъектно-объектной модели ЭС, воспользуемся следующими определениями [3].

Определение 1. Объект O_i называется источником для субъекта S_k , если существует субъект S_j , в результате воздействия которого на объект O_i в ЭС возникает субъект S_k . Субъект S_k назовем порожденным субъектом.

Определение 2. Субъект S_j , порождающий новый субъект в объекте O_i , в свою очередь, называется активизирующим или порождающим субъектом для субъекта S_k .

Определение 3. Объект O_i в момент времени t ассоциирован с субъектом S_j , если субъект S_j использует информацию, содержащуюся в объекте O_i .

Использование информации можно объяснить, анализируя процедуры взаимодействия субъектов доступа и объектов. Результат показывает, что ассоциированные объекты могут быть разделены на два вида: функционально-ассоциированные объекты и ассоциированные объекты-данные.

Функционально-ассоциированные объекты определяют содержание процедуры воздействия субъекта. Например, микропрограммы в программируемых устройствах определяют свойства субъекта в следующий момент времени. Другой пример, состояние контактов матрицы клавиатуры (замкнуты, разомкнуты) влияет на функции, выполняемые контроллером клавиатуры. Таким образом, матрица клавиатуры является функционально ассоциированным объектом для субъекта – контроллер клавиатуры.

Ассоциированные объекты-данные выступают в роли аргументов в операциях, порождающих потоки информации (например, регистры состояний в устройствах управления).

Множество ассоциированных объектов O_j с субъектом S_i в момент времени t обозначим, как

$$S_i(\{O_j\}t).$$

Активная сущность субъектов доступа заключается в их возможности осуществлять определенные действия над объектами, что объективно приводит к возникновению потоков информации.

Формализуем механизм доступа с целью порождения нового субъекта. Расширим понятие доступа и уточним его модель, приведенную в [4].

Введем операцию:

$$\text{Create}(S_j, O_i, P') \rightarrow S_k, \quad (1)$$

которая означает, что при воздействии субъекта S_j , с помощью активизирующего потока команд P' , на объект O_i порожден субъект S_k . *Create* назовем операцией порождения субъектов.

Отметим, что ввиду того, что в ЭС 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. В том случае, когда при воздействии субъекта S_j , с помощью активизирующего потока P' , на объект O_i порождение субъекта S_k не происходит $\text{Create}(S_j, O_i, P') \rightarrow \emptyset$.

Если субъект S_j играет роль нарушителя S_0 , а субъект S_k – роль ИУ (S^*), тогда процесс активизации ИУ описывается следующей образом [1]:

$$\text{Create}(S_0, O_i, P'_{unsp}) \rightarrow S^*, \quad (2)$$

где поток P'_{unsp} обозначает поток неспецифицированных команд. Поток P'_{unsp} может быть порожден либо внешним субъектом нарушителя S_0 , либо внутренним механизмом активации ИУ.

Теперь формализуем механизм доступа с целью реализации обмена информацией между объектами. По определению, объекты системы являются пассивными сущностями. Для выполнения операции обмена информацией между ними, необходимо существование потоков данных от одного объекта к другому. Приведем определение потока.

Определение 4. Поток информации между объектом O_i и объектом O_j называется операция по обмену данных над объектом O_i , реализуемая субъектом S_k , и зависящая от объекта O_j .

Таким образом, порождение потока информации между объектом O_i (объект-источник) и объектом O_j (объект-получатель) всегда реализуется двумя операциями. Сначала субъект S_j порождает (активизирует) субъект S_k в объекте O_i (1). После этого поток данных P'' от объекта O_i к объекту O_j порождается операцией:

$$\text{Stream}(S_k, O_i, P'') \rightarrow O_j. \quad (3)$$

Stream назовем операцией порождения потока (или обмена информацией между объектами).

Потоки могут создаваться различными типами операций: чтение, изменение, удаление, создание и т. д. Объекты O_i и O_j , участвующие в организации потока, могут быть как источниками, так и приемниками информации, могут быть как ассоциированными, так и неассоциированными с субъектом S_k . Следует особо подчеркнуть, что согласно определению 4, потоки информации могут быть только между объектами, а не между субъектом и объектом. Это объясняется тем, что субъект это активная сущность, т. е. действия, процессы, а информация это пассивная сущность, которая может размещаться,

извлекаться, порождаться, изменяться только в объектах.

Активная роль субъекта заключается в самой реализации потока, через задействование в потоке ассоциированных с субъектом объектов (например, буферов оперативной памяти, регистров). Поток P'' может быть массивом, адресом и т.д.

Подведем итог. Механизм доступа с целью реализации обмена информацией между объектами описывается двумя операциями: операцией порождения субъекта (1) и операцией порождения потока (3):

$$\begin{aligned} \text{Create}(S_j, O_i, P') &\rightarrow S_k, \\ \text{Stream}(S_k, O_i, P'') &\rightarrow O_j. \end{aligned} \quad (4)$$

Предположим, что субъект S_j играет роль нарушителя S_0 , а субъект S_k – роль ИУ S^* , тогда модель несанкционированного доступа с целью реализации обмена информацией между объектами в этом случае, имеет вид:

$$\begin{aligned} \text{Create}(S_0, O_j, P'_{unsp}) &\rightarrow S^*, \\ \text{Stream}(S^*, O_j, P''_{unsp}) &\rightarrow O_m. \end{aligned} \quad (5)$$

Анализируя модель несанкционированного доступа (5) приходим к важному выводу: для обеспечения гарантированного выполнения заданной политики безопасности (ПБ) в ЭС нужно контролировать не только факт несанкционированного доступа субъекта к объекту в виде потоков P'_{unsp} , но и неспецифицированные потоки данных P''_{unsp} .

На основании изложенного, введем определение доступа, которое занимает центральное место в политике и моделях разграничения доступа.

Определение 5. Доступом называется операция обращения субъекта S_k к объекту O_i с целью порождения нового субъекта и/или реализации обмена информацией между объектами O_i и O_j .

Если принять во внимание, что создание субъекта всегда преследует цель выполнения определенных действий над информацией, то можно констатировать, что доступ – это, в общем случае, двухэтапная процедура. Это влечет за собой следующее заключение: модель доступа включает потоки не только между объектами, но и между субъектами и объектами.

Формальное определение доступа (4) дает возможность средствами субъектно-объектной модели перейти непосредственно к описанию процессов безопасности информации в защищенных ЭС.

3. ПОТОКИ И ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА СУБЪЕКТОВ К ОБЪЕКТАМ

Рассмотрим множество потоков P для всей совокупности фиксированных декомпозиций ЭС на субъекты и объекты во все моменты времени. С точки зрения безопасности, трактуемой

как состояние защищенности информации в ЭС, множество потоков P разбивается на два непересекающихся подмножества P_{AU} и P_{UNAU} :

$$P = P_{AU} \cup P_{UNAU}, \\ P_{AU} \cap P_{UNAU} = \emptyset,$$

где P_{AU} – множество потоков, вызываемых разрешенными (authorized); P_{UNAU} – множество неразрешенных (unauthorized), нарушающих состояние защищенности информации.

Потоки P_{AU} и P_{UNAU} могут быть представлены двумя подмножествами. Так,

$$P_{AU} = P' \cup P'',$$

где P' – специфицированный поток команд, P'' – специфицированный поток данных, а

$$P_{UNAU} = P'_{unsp} \cup P''_{unsp},$$

где P'_{unsp} – несанкционированный поток команд, P''_{unsp} – неспецифицированный поток данных.

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

Определение 6. Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие множеству P_{AU} .

Это определение является фундаментальным положением субъектно-объектной модели ЭС, на котором будут строиться 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 6 не конкретизирует и не детализирует конкретных механизмов фильтрации потоков на санкционированные и несанкционированные, то можно говорить, что субъектно-объектная модель доступа ЭС инвариантна относительно любой принимаемой в ЭС политики безопасности.

4. МОНИТОР БЕЗОПАСНОСТИ ЭС

В данном разделе рассмотрим понятие и роль монитора безопасности ЭС, а также основы построения моделей безопасности схемного уровня.

Анализируя основные положения субъектно-объектной модели системы, касающиеся структуры и функционирования защищенных систем [3], сформулируем аналогичные аксиоматические условия для защищенных ЭС.

Аксиома 1. В защищенной ЭС в любой момент времени любой субъект и объект должны быть идентифицированы и аутентифицированы.

Данная аксиома реализуется самой процедурой проектирования и содержанием процессов функционирования ЭС. Так, для ЭС специфицированные объекты и субъекты, а также топология системы, определяются технической документа-

цией. Аксиома 1 выражает **необходимое условие безопасности (защищенности) информации в ЭС.**

Аксиома 2. В защищенной ЭС должна присутствовать активная компонента (субъект) с соответствующим объектом-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам.

В [2, 3] для данной активной компоненты утвердился термин «монитор безопасности» (МБ). Это понятие связано с упоминаемой выше задачей фильтрации потоков. Целевая функция МБ – фильтрация потоков с целью обеспечения безопасности ЭС. В защищенной ЭС появляется дополнительная компонента, обеспечивающая управление доступом на основе той или иной политики безопасности.

В виду того, что связи между объектами и субъектами, а также процессы обработки информации устанавливаются на этапе проектирования ЭС, то МБ безопасности должен быть интегрирован непосредственно в систему (в ее ядро) на этапе проектирования. Очевидно, что в рассматриваемом случае МБ реализуется на нулевом (hardware) уровне представления системы и управляет доступом на этом уровне. Наиболее эффективной является стратегия, заключающаяся в такой разработке компонентов ЭС, включая МБ, которая бы изначально строилась на основе определенной модели разграничения доступа.

Таким образом, именно МБ в защищенной ЭС является субъектом осуществления принятой политики безопасности, реализуя ее через алгоритмы своей работы, которые соответствуют модели безопасности. В этом отношении большое значение имеет следующее аксиоматическое положение [3], расширенное для случая ЭС.

Следствие 1 (из аксиомы 2). В защищенной ЭС существует особая категория субъектов (активных сущностей), которые не инициализируют другие субъекты и к которым отсутствует доступ пользователя (нарушителя).

Это системные субъекты (процессы), присутствующие (функционирующие) в системе изначально. К числу подобных системных субъектов относится МБ, который управляет доступами субъектов (в том числе и пользователей) к объектам системы. Следовательно, для обеспечения защищенности в ЭС свойства системных субъектов должны быть неизменными, от чего напрямую зависят гарантии безопасности.

Аксиома 3. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима (должна существовать) дополнительная информация и объекты, ее содержащие.

Из аксиомы 3 следует, что МБ, в свою очередь, как и любая активная сущность в ЭС, является субъектом с соответствующим объектом-источником и ассоциированными объектами. Отсюда вытекают следующие важные следствия.

Следствие 2 (из аксиомы 3). Ассоциированный с монитором безопасности объект, содержащий информацию о системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационных ресурсов в защищенной ЭС.

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

Информация в ассоциированном с монитором безопасности объекте должна касаться специфицированных субъектов и объектов системы, а также топологии системы. Следовательно, для планирования и управления системой разграничения доступа ЭС должна быть предусмотрена процедура доступа к данному объекту со стороны внешней среды, т. е. через субъекты пользователя. Отсюда вытекает еще одно следствие.

Следствие 3 (из аксиомы 3). В защищенной системе может существовать **доверенный пользователь (системный администратор)**, субъекты которого имеют доступ только к ассоциированному с монитором безопасности объекту для управления политикой разграничения доступа. Эти субъекты не должны иметь доступ к элементам или процессам монитора безопасности.

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

В практическом плане, к реализации монитора безопасности ЭС, предъявляются следующие обязательные требования:

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

2. Если предположить, что ИУ может воспользоваться штатным каналом ЭС, т.е. каналом, который поддерживает потоки из множества P_{AU} , становится очевидным необходимость осуществления контроля всех потоков в каналах связи.

3. Изолированность. МБ должен быть защищен от отслеживания и перехвата своей работы.

4. Верифицируемость. МБ должен быть проверяемым (само- или внешне тестируемым) на предмет выполнения своих функций.

5. Непрерывность. МБ должен функционировать при любых штатных и нештатных, в том числе и аварийных ситуациях.

6. Механизм управления доступом должен гарантированно реализовывать заданную политику безопасности.

7. Механизм управления доступом не должен влиять на качество выполнения ЭС основных функций.

Включение в архитектуру ЭС специального субъекта для мониторинга должно обеспечивать конфиденциальность, целостность и доступность информации.

5. ОБЕСПЕЧЕНИЕ ГАРАНТИЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ЭС

Целью данного подраздела является разработка критериев гарантированной безопасности ЭС.

Как правило, модели, связанные с реализацией политики безопасности [2, 5, 6], не учитывают возможности субъектов по изменению самой системы, которые могут привести к изменению её свойств, и как предельный случай, к полной неприменимости той или иной модели к описанию отношений «субъект-объект» уже в измененной системе. Поэтому вопрос гарантий политики безопасности является ключевым как в теории, так и в практике.

Рассматривая активную роль субъектов (в том числе и ИУ) в ЭС, необходимо отметить ряд важнейших их свойств, на которых базируются излагаемые ниже гарантии безопасности.

Во-первых, необходимо заметить, что человек-пользователь воспринимает объекты и получает информацию о состоянии ЭС через субъекты, которыми он управляет и которые производят отображение информации в воспринимаемом человеком виде.

Во-вторых, угрозы компонентам ЭС исходят от субъектов как активной компоненты, порождающей потоки и изменяющей состояние объектов в КС.

В-третьих, субъекты могут влиять друг на друга через изменяемые ими объекты, связанные с другими субъектами, порождая в конечном итоге в системе субъекты (или состояния системы), которые представляют угрозу для безопасности информации или для работоспособности самой системы

В-четвертых, субъекты, которые представляют угрозу для безопасности информации, могут использовать штатные каналы системы.

Положения субъектно-объектной модели системы, а также, понятия доступа субъектов к объектам и политики безопасности позволяют сформулировать следующий общий критерий безопасности системы [2, 3].

Определение 7. Электронная 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 (МБ). Его наличие в структуре ЭС является необходимым условием безопасности. Что касается условий достаточности, то, очевидно, они заключены, несмотря на тавтологию выражения, прежде всего, в безопасности самого МБ.

В практической реализации выполнение данного требования, с учетом определения доступа, приводит к необходимости разделения МБ на два отдельных субъекта: монитор безопасности объектов (МБО); монитор безопасности субъектов (МБС). Введем соответствующие определения.

Определение 8. Монитором безопасности объектов называется субъект, активизирующийся при возникновении потока, порожаемого любым субъектом, между любыми объектами и разрешающий только те потоки, которые принадлежат множеству P'' . МБО должен фильтровать те потоки, которые принадлежат множеству P''_{unsp} .

Определение 8, по сути, вводит в состав политики безопасности ЭС, в качестве дополнительной составной части, специальную политику относительно потоков информации между объектами.

Определение 9. Монитором безопасности субъектов называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов из фиксированного подмножества пар активизирующих субъектов и объектов-источников.

МБС разрешает только те потоки, которые принадлежат множеству P' . МБС должен фильтровать те потоки, которые принадлежат множеству P'_{unsp} .

Определение 9, практически, вводит в состав политики безопасности ЭС в качестве дополнительной составной части специальную политику относительно порождения субъектов доступа.

Как и у любого субъекта, у МБС должен быть объект-источник, функционально-ассоциированный объект, включающий, например, программируемый модуль и ассоциированный объект-данные, содержащий необходимую информацию по политике порождения субъектов доступа в системе (рис. 1).

Атаки некоторых типов ИУ [1,7] осуществляются по сценарию подмены функций специфицированных субъектов (т. е. фактически

подмены свойств субъектов) или возникновение нового неспецифицированного субъекта. Поэтому важным аспектом, с точки зрения гарантий выполнения политики безопасности, является **неизменность свойств субъектов** доступа в процессе функционирования ЭС. Данное требование имеет отношение к любым субъектам доступа, но особо для субъектов МБ.

Для построения доказательной базы защищенности информации в ЭС рассмотрим следующие понятия: тождественность объектов, а также тождественность и неизменность субъектов.

Определение 7. Объекты O_i и O_j в момент времени t тождественны ($O_i(t) \equiv O_j(t)$), если они совпадают как структура, так и как слова, записанные в одном языке в памяти.

В частном случае, когда ($O_i(t_1) \equiv O_i(t_2)$) $t_1 \neq t_2$, будем говорить о тождественности одного и того же объекта в разные моменты времени.

Тождественность объектов по определению 7 основывается как на физической (структурной) тождественности, так и на тождественности уровня последовательности символов из алфавита языка представления [3, 5]. Введенное понятие тождественности объектов позволяет перейти к рассмотрению понятия тождественности и неизменности субъектов доступа.

Определение 8. Субъекты S_i и S_j тождественны в момент времени t , если попарно тождественны все ассоциированные с ними объекты.

В общем случае, определения 7 и 8 неявно требуют наличия в системе специального механизма сортировки однотипных объектов и их попарного сравнения. В электронных системах тождественность объектов, а также тождественность и неизменность субъектов выполняются априорно за счет неизменности электрических соединений и функциональной спецификации, реализованной на этапе проектирования. Это обуславливает следующее следствие.

Следствие 4 (из определений 7 и 8). В электронных системах тождественность объектов, а также тождественность и неизменность субъек-

Защищенная ЭС

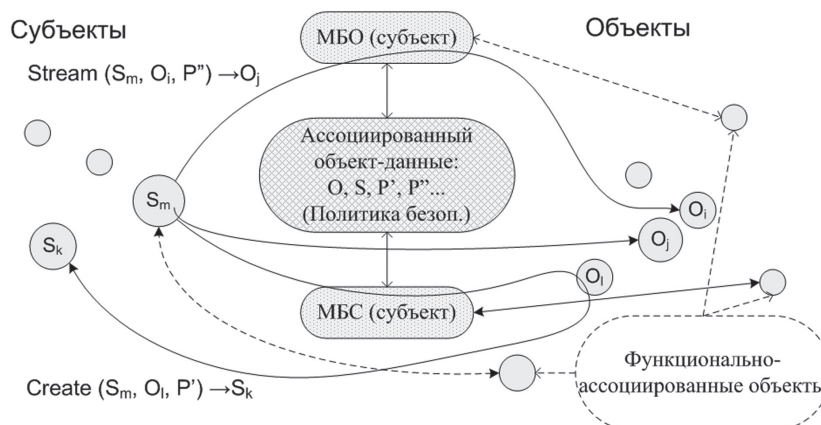


Рис. 1. Порождение потоков (Stream) и субъектов (Create) с учетом МБО и МБС

тов обеспечивается фильтрацией (блокировкой) потоков P'_{unsp} .

Рассмотрим объект O_i , который содержит ИУ. Сравним этот объект O_i в момент времени t , когда ИУ находится в пассивном состоянии, с этим же объектом O_i в момент времени $t+1$, когда ИУ находится в активном состоянии. Будучи физически тождественными в момент времени t , эти объекты стали физически не тождественными после активизации ИУ в момент времени $t+1$. Сделаем вывод: отсутствие потока P'_{unsp} в момент времени t гарантирует тождественность объектов в момент времени $t+1$, а, следовательно, гарантирует отсутствие угроз, исходящих от ИУ, и появление потоков P''_{unsp} . Исключением является случай автономной активизации или активизации с помощью беспроводного канала.

Следствие 5 (из определений 7 и 8). Порожденные субъекты тождественны, если тождественны все порождающие субъекты и объекты-источники.

Обоснованность данного следствия вытекает из тождественности 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 9. Субъекты S_i и S_j называются не влияющими друг на друга (или корректными относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами O_i и O_j , ассоциированными, соответственно с субъектами S_i и S_j . Причем объекты O_i не ассоциированы с субъектом S_j , а объекты O_j не ассоциированы с субъектом S_i .

Отметим, что термин «изменение состояния объекта» в определении 9 трактуется как нетождественность (в смысле определения 7) объекта с самим собой в различные моменты времени. При этом подчеркивается, что операция изменения объекта локализована в субъекте, с которым этот субъект не ассоциирован. Очевидно, что в ЭС эта нетождественность порождается потоками P'_{unsp} или P''_{unsp} .

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

Определение 10. Субъекты S_i и S_j называются абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если в условиях определения 9 множества ассо-

циированных объектов указанных субъектов не имеют пересечения.

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

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

Доказательство. Из условия абсолютной корректности любых субъектов с МБО вытекает отсутствие потоков P''_{unsp} , которые могут изменить функционально-ассоциированные и ассоциированные объекты-данные МБО и тем самым изменить его свойства для осуществления обхода (нарушения) политики безопасности.

С другой стороны, такие потоки могут появиться при изменении ассоциированных объектов, принадлежащих другим субъектам ЭС для возможного нарушения (обхода) политики безопасности. Условие корректности субъектов относительно друг друга делает это невозможным (по определению абсолютной корректности). Это в свою очередь означает, что МБО реализует только потоки из множества P'' . Тем самым **утверждение доказано**.

Утверждение 1 для обеспечения гарантий безопасности накладывает чрезвычайно жесткие и труднореализуемые на практике условия. Кроме того, невозможно гарантировать корректность любого субъекта, активизируемого в ЭС (особенно в случае автономной активизации ИУ), относительно МБО. Очевидно, что эти условия существенно снижают функциональные возможности ЭС (фактически, это требование отсутствия общих ассоциированных объектов-данных, например, регистров состояния, буферов для обмена данными, а также ассоциированных объектов источников, например, МП для субъектов).

С практической точки зрения, наиболее логичными и интересными являются подходы, позволяющие уменьшить число объектов и субъектов, которые охватываются политикой безопасности. При проектировании ЭС всегда можно гарантированно обеспечить сокращение множества возможных порождаемых субъектов до некоторого подмножества фиксированной мощности, при этом, не гарантируя отсутствия некорректных субъектов внутри этого подмножества.

Отметим, что в сформированное подмножество субъектов в момент времени t включается и МБС. Поэтому, первым аргументом операции Create может быть только субъект, входящий в подмножество субъектов, а аргумент-объект, вообще говоря, любым.

Для демонстрации этого подхода введем понятия замкнутости и изолированности подмножества субъектов системы.

Определение 11. ЭС 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 ЭС на субъекты и объекты.

Согласно этому определению подмножество субъектов может включать некорректные субъекты, т.к. объекты-источники могут быть и не нетождественными относительно друг друга.

Для описания системы в части защищенности, свойство замкнутости ЭС по порождению субъектов необходимо дополнить свойством изолированности.

Определение 12. Множество субъектов ЭС называется изолированным (абсолютно изолированным), если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

Таким образом, механизм замкнутой по порождению субъектов ЭС и свойство изолированности множества субъектов сокращает множество возможных порождаемых субъектов до некоторого подмножества фиксированной мощности, при этом, не гарантируя отсутствия некорректных субъектов внутри замкнутой среды.

Из определения 12 вытекают следующие следствия.

Следствие 6 (из определения 12). Любое подмножество субъектов изолированной (абсолютно изолированной) ЭС, включающее МБС, также составляет изолированную (абсолютно изолированную) среду.

Следствие 7 (из определения 12). Дополнение изолированной (абсолютно изолированной) среды субъектом, корректным (абсолютно корректным) относительно любого субъекта 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 2 (достаточное условие гарантий безопасности 2). Если в абсолютно изолированной ЭС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также существует МБС, который абсолютно корректен относительно МБО, то в ЭС реализуется только доступ, описанный политикой разграничения доступа.

Доказательство. По определению 12 и следствиям из него в системе могут существовать только абсолютно корректные относительно МБС и друг друга субъекты из некоторого их конечного множества. Следовательно, отсутствует возможность изменения свойств МБС. Абсолютная корректность МБС и других субъектов по отношению к МБО обеспечивает отсут-

ствии возможностей изменения свойств МБО, что в итоге автоматически обеспечивает разрешение только тех потоков, которые входят в множество $P_{AU} = P' \cup P''$. Утверждение **доказано**.

В отличие от первого условия достаточности гарантий выполнения политики безопасности, когда требовалась корректность МБО относительно произвольного субъекта, второе условие менее жестко, т. к. накладывает условия абсолютной корректности не на все множество возможных субъектов, а лишь на фиксированное их подмножество, образующее замкнутую аппаратную среду. 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 изолированной ЭС, показал необходимость включения требований по неизменности свойств объектов, связанных с процедурами порождения субъектов.

При технической реализации операции Create по порождению субъектов, которые составляют изолированную среду в ЭС, возникает весьма важная проблема, связанная с тем, что в реальной ЭС один и тот же объект может иметь различные состояния во времени (например, безопасные или опасные). Предположим, что зафиксировано состояние объекта O_i в некоторый момент времени t_0 . Обозначим состояние объекта O_i в момент времени t как $O_i(t)$.

Определение 13. Операция порождения субъектов $Create(S_j, O_i, P) \rightarrow S_k$, называется порождением с контролем неизменности объекта, если для любого момента времени $t > t_0$, в который активизирована операция порождения субъекта Create, порождение субъекта S_k возможно только при тождественности объекта-источника относительно момента t_0 , т. е. при $O_m(t) \equiv O_m(t_0)$.

Из определения 13 вытекает следующее важное следствие, имеющее непосредственное отношение к неизменности свойств субъектов доступа, как важнейшего условия обеспечения политики безопасности в системе.

Следствие 8 (из определения 13). В условиях определения 13 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 субъект.

Введение понятия порождения субъектов с контролем неизменности объектов позволяет сформулировать и доказать такое достаточное условие для обеспечения замкнутой ЭС, которое во-первых, может быть практически реализовано в реальных ЭС, а во-вторых, сделать безопасной траекторию состояний ЭС.

Утверждение 3. (базовая теорема изолированной ЭС). Если в момент времени t_0 в изолированной ЭС действует только порождение

субъектов с контролем неизменности объекта, и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени $t > t_0$ ЭС также остается изолированной (абсолютно изолированной).

Доказательство. Условие корректности для потоков в начальный момент t_0 времени функционирования системы обеспечивает исходную «безопасность» всех объектов-источников для последующего порождения субъектов системы, порождением с контролем неизменности объекта.

По условию утверждения 3 в ЭС возможно существование потоков, изменяющих состояние объектов, не ассоциированных в этот момент времени с каким-либо субъектом. Если объект с измененным состоянием не является источником для порождения субъекта, то множество субъектов изолированной среды нерасширяемо, в противном случае (измененный объект является источником для порождения субъекта с нарушением условия «контроля неизменности объекта») по условиям утверждения (порождение субъекта с контролем) порождение субъекта невозможно. Следовательно, мощность множества субъектов не может превышать той, которая была зафиксирована до изменения состояния любого объекта. Таки образом, множество субъектов ЭС остается изолированным и любой момент времени будут соблюдаться требования изолированности ЭС. Утверждение доказано.

ВЫВОДЫ

1. Утверждения 1–3 имеют важное значение с точки зрения достаточных условий для обеспечения гарантий выполнения политики безопасности в защищенных ЭС, т.к. позволяют сформулировать методологию проектирования гарантировано защищенных ЭС.

2. Теоретические результаты, полученные в работе, создают **инвариантную основу** по отношению к любым политикам и моделям разграничения доступа для гарантий выполнения политики безопасности в защищенных ЭС.

3. Вместе с тем, не рассмотрена ситуация, связанная с автономной активацией ИУ и активацией с помощью беспроводного канала.

4. При практической реализации условий утверждения 3 возникает несколько серьезных проблем. Одна из них связана с исходным состоянием ЭС, в котором должны быть только потоки, гарантирующие корректность исходных субъектов. Вторая проблема связана с понижением производительности (быстродействия) ЭС в связи с выполнением процедур контроля мониторингом безопасности.

Литература

- [1] Горбачев В.А. Иванисенко И.Н. Классификация и формальные модели аппаратных закладных устройств. Прикладна радіоелектроніка та інформатика, Харьков: ХТУРЭ. — Т. 6, 2007. № 2. — С. 306–310.
- [2] Bishop M. Computer Security: art and science. Addison Wesley.
- [3] Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Уральский государственный университет им. А.М. Горького, Екатеринбург, 2008.
- [4] Горбачев В.А. Формальные основы методов блокирования аппаратных закладных устройств// Прикладна радіоелектроніка, науч.-техн. журнал, Харьков: ХНУРЭ. — Т. 11, 2012. № 2. — С. 275–280.
- [5] Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. — М.: Изд. центр «Академия», 2005. — 144 с.
- [6] Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем — М.: Телеком, 2000. — 452 с.
- [7] Benjamin Sanno, Detecting Hardware Trojans, Matrikelnummer: 108006248774 benjamin.sanno@rub.de Semester 6 Ruhr-University Bochum, Germany July 22, 2009.

Поступила в редколлегию 3.06.2014



Горбачев Валерий Александрович, профессор кафедры ЭВМ ХНУРЭ. Научные интересы: системный анализ.

УДК 638.235.231

Достатні умови безпеки інформації в електронних системах / В.О. Горбачов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 319–327.

Розглядається суб'єктно-об'єктна модель доступу, аксіоматичні достатні умови захищеності інформації, а також вимоги до монітора безпеки в електронних системах.

Ключові слова: політика безпеки, модель доступу, розмежування доступу, монітор безпеки, електронна система.

Л.: 1. Бібліогр.: 7 найм.

UDC 638.235.231

Sufficient conditions of information security in electronic systems / V.A. Gorbachov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 319–327.

A subject-object access model, axiomatic sufficient conditions of information security as well as requirements specified to security monitors in electronic systems are considered.

Keywords: security policy, access model, access isolation, security monitor, electronic system.

Fig. 1. Ref.: 7 items.