УДК 681.3

МОДЕЛИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КРИТИЧНЫХ ИНФОРМАЦИОННО - ИЗМЕРИТЕЛЬНЫХ СИСТЕМ

(Часть 1. Введение и общая модель)

Артамонов В.А.

Белорусский национальный технический университет, Минск, Республика Беларусь

Обозначена проблема построения безопасности информационных технологий критичных информационно-измерительных систем. Рассмотрены основные математические методы, применяемые при формальном анализе и описании таких систем. Вводится общая модель безопасности информационных технологий.

Введение

Информационные технологии (ИТ) становятся на сегодняшний день краеугольным камнем построения современных информационно-измерительных систем (ИИС). Вместе с этим, ИТ привнесли в эту сферу проблемы обеспечения известной "триады" – *конфиденциальности, целостности и доступности.* Таким образом, для обеспечения и поддержания режима информационной безопасности (ИБ) современных ИИС требуется разработка и реализация ***политик безопасности,*** используемых информационных технологий. В связи с этим рассмотрим основные математические методы, применяемые при формальном анализе и описании политик безопасности ИИС. При анализе функционирования этих систем (при этом системы являются необязательно вычислительными), область применения которых является критичной в плане обеспечения их жизнедеятельности (к данному классу обычно относятся защищенные ИИС), желательно рассмотреть ее реакции на все возможные входные воздействия.

Хотя количество всех возможных реакций системы достаточно велико, существует два метода, позволяющих уменьшить количество состояний, которые необходимо подвергнуть анализу.

Один из методов заключается в доказательстве того, что система всегда *"работает корректно*", тогда как альтернативный метод состоит в демонстрации того, что система *"никогда не выполняет неверных действий".*

При использовании *первого* метода используется комбинация анализа и эмпирического тестирования для определения таких реакций системы, которые могут привести к серьезным сбоям – например, функционирование системы при граничных

условиях или при условиях, не оговоренных в качестве возможных для компонентов системы. В качестве примера можно привести требование описания поведения системы в ответ на входное воздействие типа *"выключение питания"*.

Основной идеей *второго* метода является гипотеза о том, что система делает что-то некорректное, поэтому ведется анализ реакций системы с выявлением состояний, в которых возможно проявление данной некорректности. Доказательство корректности работы системы сводится к демонстрации того, что данные состояния недостижимы, то есть к доказательству от противного.

Свойство, характерное как для одной, так и для другой технологии анализа безопасности ИИС, выражаются путём группирования схожих реакций системы *(сигнатур)* так, что для рассмотрения всех возможных реакций ИИС необходимо анализировать лишь небольшое количество входных воздействий.

Данные методы анализа безопасности систем пригодны в основном для измерительных систем, основывающихся на механических, электрических и других компонентах, то есть компонентах, основанных на физических принципах действия. В системах, основанных на физических принципах, отношения между входными и выходными данными являются *непрерывными*, то есть незначительные изменения во входных данных влекут незначительные изменения в выходных данных.

Это позволяет проанализировать (протестировать) поведение системы, основанной на физических законах конечным количеством тестов, так как непрерывный характер правил функционирования системы позволяет заключить, что отклик системы на непротестированное значение входной величины будет схожим с соответствующими протестированными случаями.

Таким образом, можно сделать вывод о том, что метод непосредственного тестирования хотя и необходимо применять к системам критического назначения, но он способен выявлять только примитивные ошибки в программном обеспечении. Вследствие сложности современных программных систем и вытекающего из этого многообразия реакций системы на входной поток данных, описанная выше техника недостаточна для анализа сложных ИИС.

Общая модель

Сложность системы ИТ определяется большим количеством дискретных решений, принимаемых системой при исполнении программного обеспечения. Таким образом, при определении взаимоотношений между входом и выходом системы (входным и выходным

потоками данных), в случае анализа программной системы, реакцию системы на входное воздействие нельзя рассматривать как непрерывную функцию, так как она является дискретной: небольшие изменения во входных данных системы могут радикально изменить поведение всей системы в целом. Это является главным отличием современных ИИС от систем, основанных на физических процессах.

Отклонение от непрерывности ведет к непредсказуемому росту количества возможных реакций системы на изменения во входных данных. Таким образом, *в случае с ИИС в состав которых входят системы (подсистемы) ИТ, метод непосредственного тестирования с последующими выводами о свойствах данной системы не дает должной уверенности в её безопасности вследствие дискретного характера отношений между входными данными и выходной реакцией системы*. И таким образом, практическое значение применения формальных методов при анализе систем заключается в возможности анализа всех реакций систем ИТ.

Необходимо отметить, что в случае формального анализа мы имеем дело не просто с реакцией системы на некоторые группы входных данных, а с *внутренней реализацией системы*. Таким образом, возникает возможность "декомпозиции" возможных реакций системы на реакции ее компонентов (с помощью анализа формальных спецификаций компонентов) с последующей их композицией, что дает возможность описания всех реакций системы.

Описанные выше принципы применения формальных методов для анализа систем, содержащих программное обеспечение, имеют недостаток, присущий всем методам моделирования: *формальные методы имеют дело не с самой системой, а с ее моделью* и это означает, что модель может не отражать реальность или отражать ее некорректно.

Данная проблема может возникнуть вследствие использования модели, учитывающей не все факторы, оказывающие влияние на реальную систему. С другой стороны, излишняя детализация системы ведёт к росту затрат на проведение формального анализа, что может привести к неэффективности применения данного метода. К модели безопасности должны предъявляться требования, общие для всех моделей, а именно: *адекватность, предсказуемость, общность*. Таким образом, возникает задача корректного выбора уровня абстракции в описании модели безопасности. Под уровнем абстракции понимается множество требований к реальной системе, которые должны найти свое отражение в модели, для корректного отображения моделируемой системы.

Для того чтобы перейти к рассмотрению модели безопасности системы, рассмотрим концепцию *ядра безопасности*, отражающую свойства механизмов безопасности. В

данной концепции сеанс работы пользователя в системе ИТ характеризуется последовательностью операций доступа к объектам системы. Очевидно, что должна существовать некая процедура принятия решений о том, какой из запрашиваемых доступов разрешить, а какой нет. По другому это можно представить как фильтр, через который должны пройти все запросы на доступ, сделанные *субъектами*. Схема такого фильтра получила название *монитора пересылок* (возможная реализация в виде программной и /или аппаратной компоненты) .

Основной характеристикой монитора пересылок является то, что он или разрешает запрос на доступ, или запрещает, возможно, уведомляя об этом субъекта. Таким образом, монитор пересылок может быть описан в терминах функции с запросами на обслуживание, разрешениями доступа, другими компонентами состояния системы на входе (т. е. элементами области определения) и разрешениями или запретами на обслуживание на выходе (т. е. элементами области значения).

Монитор пересылок должен удовлетворять следующим основным требованиям:

-ни один запрос на доступ субъекта к объекту не должен проходить мимо монитора пересылок

-целостность монитора пересылок должна строго контролироваться;

-представление монитора пересылок должно быть достаточно простым для доказательства корректности его работы.

Однако совершенно необязательно, чтобы безопасная система включала в свою архитектуру отдельный модуль (возможно, называемый модулем монитора пересылок), который бы обрабатывал запросы. Способ выполнения обработки запросов определяется проектировщиками и разработчиками системы.

На уровне рассмотрения системы в целом, свойства безопасности системы являются функцией свойств безопасности ядра безопасности системы.

В математической логике существует понятие предикатов первого и второго порядка [1]. Предикаты второго порядка расширяют предикаты первого порядка в том, что они позволяют осуществлять применение логических операторов *общности* **(∀)** и *существования* **(∃)** не только над переменными, но и над функциями.

Многие свойства систем могут быть выражены в терминах логики первого порядка, например, свойство стека системы может быть описано следующим предикатом первого порядка: **∀x top (push (s, x)) = x**.

Логика первого порядка определяет свойство того, что система делает. Однако, для описания свойств безопасности системы необходимо применение логики второго

порядка. Ядро безопасности гарантирует безопасность системы вне зависимости от того, какие его функции и в какой последовательности задействованы. При этом свойства безопасности системы в целом могут быть описаны следующим выражением :

$$\forall \alpha \in op' : P(\alpha), \qquad (1)$$

где **op'**- множество всех возможных последовательностей вызовов функций, предоставляемых ядром безопасности системы;

P() - предикат, определяющий выходную реакцию в системе в зависимости от входного воздействия.

Выражение (1) является предикатом второго порядка и определяет следующее свойство: *любая операция, выполняемая пользовательским программным обеспечением, преобразуется в последовательность вызовов функций ядра безопасности системы (функций в множестве **op'**) и при условии защиты программного обеспечения ядра системы от модификации, свойство **P()** является свойством системы в целом (данное свойство не зависит от поведения программного обеспечения, не принадлежащего ядру системы).* Доказательство безопасности системы сводится к демонстрации инвариантности модели системы по отношению к некоторому свойству безопасности, определяемому предикатом **P**. В анализируемых моделях безопасности предикат **P** конкретизируется и вместо исследования выражений, описываемых логикой второго порядка, исследуются состояния системы.

Таким образом, д*ля модели ИИС, в составе которой присутствуют системы ИТ сформулируем основное **утверждение**, которое в дальнейшем докажем в виде теорем: **"Если система начинает работу в безопасном состоянии и все переходы системы из состояния в состояние являются безопасными, то система является безопасной ".***

Для этого введём понятия, необходимые для описания свойств состояния системы: ***сущности, субъекта, объекта и доступа***, которые являются основой описания состояния моделей безопасности защищенных ИИС.

Под ***сущностью*** будем понимать любую именованную составляющую системы или продукта ИТ.

Объект будет определяться как *пассивная сущность,* используемая для хранения или получения информации. Примеры объектов: записи, блоки, страницы, сегменты, файлы, директории, биты, байты, слова, терминалы, узлы сети и т.д.

Субъект будет определяться как *активная сущность,* которая может инициировать запросы ресурсов и использовать их для выполнения каких-либо вычислительных

заданий. В процессе исполнения субъекты исполняют операции. Под субъектами мы будем обычно понимать пользователя, процесс или устройство.

Хотя основную концепцию идентификации субъектов и объектов в системе описать просто, при практической реализации часто бывает нетривиальной задачей определить: что есть субъект, а что - объект. Например, в операционной системе процессы, конечно, являются субъектами, в то время как файлы и связанные с ними директории - объектами. Однако, когда субъекты получают коммуникационные сообщения от других субъектов, встает вопрос, рассматривать ли их как субъекты или же как объекты. Данная трудность может быть преодолена путем усложнения понятия субъекта в модели.

При исполнении субъектами операций происходит взаимодействие субъектов и объектов. Такое взаимодействие называется доступом.

Доступ - это взаимодействие между субъектом и объектом, в результате которого происходит перенос информации между ними. Существуют две фундаментальные операции, переносящие информацию между субъектами и объектами. Под *операцией чтения* понимается операция, результатом которой является перенос информации от объекта к субъекту. Под *операцией записи* понимается операция, результатом которой является перенос информации от субъекта к объекту. Данные операции являются минимально необходимым базисом для описания широкого круга моделей, описывающих защищенные системы.

Рассмотрим характеристики субъектов и объектов, относящиеся к понятию безопасности. Основной характеристикой безопасности субъекта является *уровень безопасности.*

Под ***уровнем безопасности*** будем понимать иерархический атрибут, который может быть ассоциирован с сущностью ИИС для обозначения степени ее чувствительности в смысле безопасности. Данная степень чувствительности может определять, например, степень ущерба от нарушения безопасности данной сущности в ИИС. Когда в системе существуют такие иерархические отношения, то требуется некий механизм, соответствия сущности ИИС её уровню безопасности.

Для представления уровней безопасности введем математические структуры и соотношения. Обозначим множество уровней безопасности символом **L**; иерархическое отношение между различными элементами **L** описываются символами: **"<" , "≤", ">" и "≥".** Множество **L** может рассматриваться как полностью упорядоченное множество (то есть любые два элемента **L** можно сравнить для определения того, равны они между собой или какой-то из них больше другого).

Доверие определяется как атрибут, задающий чувствительность субъекта к безопасности.

С*екретность* определяется как атрибут объекта, обозначающий его чувствительность к безопасности. Эти концепции можно представить при помощи проекции субъектов и объектов на уровни безопасности посредством двух простых функций: ***clearance*** **и** ***classification***.

Областью значений каждой из функций является множество **L**. Функция ***clearance*** определена на множестве **S**, а ***classification*** определена на множестве O. Эти функции записываются в виде:

clearance: S→L

classification: O→L

Рассмотрим общие принципы построения математических моделей безопасности ИИС.

Модели безопасности ИИС состоит из двух компонентов: *системного компонента* и *компонента безопасности.* Данные компоненты находят свое отражение в характеристиках субъектов и объектов системы.

Системный компонент определяет функциональные требования к системе ИТ в контексте модели безопасности. Отсутствие или некорректное определение компонента безопасности ведет к некорректной цели анализа. И в основе всех компонентов безопасности (относятся данные модели к целостности, раскрытию или отказу в обслуживании) лежит идея о том, что доступ (по чтению, записи, исполнению и т.д.) к информации должен получать только пользователь (или процесс, действующий в его интересах), который должен быть авторизован для этого.

Компонент безопасности определяет понятие безопасности, используемое в модели. Соответствие анализируемой модели реальности определяется уровнем абстрактности системного компонента. Недостаточная детализация данного компонента ведет к тому, что модель безопасности не отражает свойства реальной системы, и как следствие, делать выводы о реальной безопасности системы на основании данной модели не предоставляется возможным. С другой стороны, чрезмерная сложность системного компонента модели ведет как к увеличению времени на формальный анализ системы, так и невозможности доказательства безопасности модели на более широкий круг систем.

Заключение

Для того, чтобы перейти к описанию моделей безопасности, необходимо обозначить принципы их построения, то есть построить их классификацию. Предлагаемая классификация моделей безопасности построена по принципу используемых в их описании понятий *субъекта и объекта*. Данная классификация отражает принципы постепенного семантического уточнения характеристик субъектов и объектов модели. Семантическое уточнение касается как уточнения особенностей описания фундаментальных операций доступа, используемых субъектами системы, так и введения в модель новых типов доступа с соответствующими ограничениями на них. Данное уточнение ведет к постепенному усложнению системного компонента модели.

Соответствующие модели отличаются компонентом безопасности и в основном совпадают в системном компоненте.

Следовательно, и это будет показано далее, доказательство безопасности соответствующих моделей будет во многом аналогично. Разница проявится в инверсии требований безопасности, что вызвано различными компонентами безопасности, принятыми в модели.

Список цитируемых источников

1.Справочная книга по математической логике: В 4-х частях/ Под ред. Дж. Барвайса.—Ч.1. Теория моделей: Пер. с англ. – М.: Наука, Главная редакция физико-математической литературы, 1982 г. – 392 с.

Artamonov V.A

THE MODELS OF SAFETY INFORMATION TECHNOLOGIES CRITICAL INFORMATION-MEASURING SYSTEMS
(Part 1. Introduction and the general model)

The problem of construction safety the information measuring systems is designated. The basic mathematical methods applied at the formal analysis and the description of such systems are considered. The general model of safety information technologies is entered.