УДК 681.326

Разработка субъектно-объектной модели системы обеспечения безопасности информации автоматизированной системы на основе ее декомпозиции

С. Н. Гончаров, А. В. Комаров, В. Б. Медведев

Представлена субъектно-объектная модель, описывающая состояния автоматизированной системы, позволяющая разделять безопасное и опасное состояния, сформулировать положения, при выполнении которых система останется в безопасном состоянии при осуществлении любых переходов. Использование субъектно-объектной модели позволяет формализовать описание политики безопасности и построить гарантированно защищенную систему.

Подход к разработке модели системы обеспечения безопасности информации

Для синтеза системы обеспечения безопасности информации использован формальный подход. Использование данного подхода позволит создать описание взаимодействия субъектов и объектов в соответствии с прохождением информационных потоков, а также выработать требования, необходимые для контроля доступа. За счет абстрагирования от особенностей архитектуры автоматизированной системы (АС) появляется возможность применения унифицированных методов обеспечения безопасности: средства управления доступом, не зависящие от политики безопасности; средства авторизации, идентификации и аутентификации, не зависящие от особенностей функционирования прикладных средств, и т. п.

Разрабатываемая модель должна учитывать особенности построения АС и характер процессов, протекающих в ней. Большое значение придается критичности информационных потоков, связанных с передачей команд управления, а также строгой аутентификации и фиксированию всех производящихся операций.

Функционирование АС строится на создании информационных потоков между компонентами системы и управления этими потоками. Система обеспечения безопасности информации должна разрешать допустимые потоки, предотвращать недопустимые потоки, обеспечивать конфиденциальность, целостность циркулирующей информации и доступность компонентов системы их легальным пользователям.

Требования к разрабатываемой модели

Задача исследований состоит в формулировании модели взаимодействия элементов АС с требованием строгого описания воздействия на объекты, в том числе в процессе передачи по каналам связи. Данная модель должна легко проецироваться на архитектуру современных АС. В рамках субъектно-ориентированной модели рассматриваются условия гарантий выполнения политики безопасности, задаваемой руководящими документами по защите информации. В системе должна реализовываться процедура принятия решений, которая определяет, разрешить запрашиваемый доступ или запретить.

Модель должна позволять разбивать взаимодействующие компоненты АС на подмножества, наделенные определенными функциями, при этом рассматривается как внутреннее, так и внешнее взаимодействие компонентов АС. Вычислительная система может быть рассмотрена в виде субъектов и объектов, взаимодействующих посредством операций, разрешение взаимодействия определяется доступом, при взаимодействии образуется информационный поток. Такую модель можно назвать субъектно-объектной. Субъектно-объектная модель описывает состояния системы, позволяет разделять безопасное и небезопасное состояния, формулировать положения, при выполнении которых система останется в безопасном состоянии при осуществлении любых переходов. Использование субъектно-объектной модели позволяет формализовать описание политики безопасности и построить гарантированно защищенную систему.

Модель субъектно-объектного взаимодействия

Модель произвольной АС в виде конечного множества элементов можно разделить на два подмножества: множество объектов и множество субъектов. Данное разделение основано на свойстве элемента сети быть активным, производить некоторые операции, получать управление. Оно исторически сложилось на основе модели вычислительной машины фон Неймана, согласно которой последовательность выполняемых инструкций (программа, соответствующая понятию "субъект") находится в единой информационной среде с данными (соответствующими понятию "объект").

Субъект является активным процессом, который способен выполнять некоторые операции над другими объектами сети, получая управление. Для порождения процесса используется некоторая информация, изначально заключенная в неактивном объекте сети: исходный код, скомпилированный исполняемый файл и т. п.

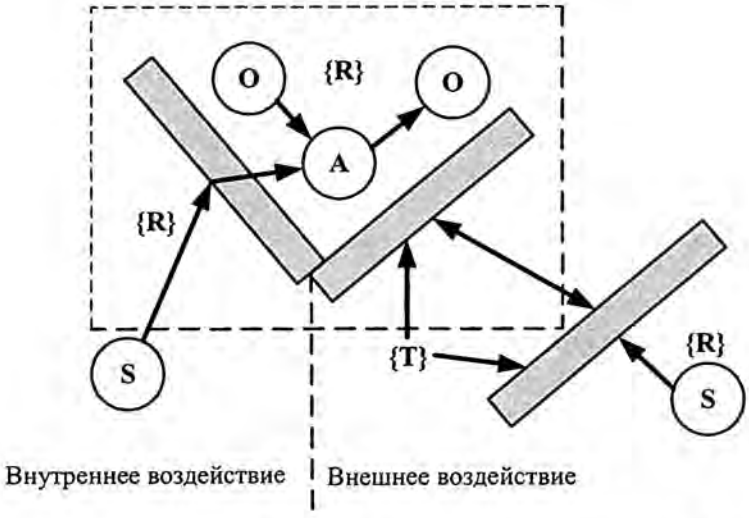
Объект – пассивная сущность вычислительной сети. В общем случае вычислительная сеть является распределенной, т. е. представляет собой комплекс различных вычислительных машин, объединенных каналами передачи данных. Субъекты и объекты такой АС располагаются на различных ЭВМ и устройствах обработки, входящих в ее состав. Сущности АС: объекты и субъекты должны однозначно идентифицироваться или иметь наименования.

В АС для каждого пользователя рассматриваются две сущности: субъект – процесс (программа), представляющий пользователя или действующего от его имени, а также сам пользователь. Вторая сущность – пассивная: объект – информация, к которой пользователь имеет санкционированный доступ.

Кроме этого существует набор административных и защитных механизмов, обслуживающих АС, поддерживающих среду для передачи, обработки и хранения информации. Они представляются отдельными субъектами. Аспекты обеспечения их безопасности, а также поддержка их функционирования не рассматриваются в проводимых исследованиях – это отдельные задачи. Считается, что данные механизмы постоянно и безотказно предоставляют системе защиты АС

необходимые функции. На рисунке представлено схематичное изображение структуры АС с точки зрения распределения компонентов сети на объекты и субъекты, при этом заштрихованными прямоугольниками обозначены барьеры защиты. На рисунке приняты следующие обозначения: **A** – администратор; **O** – объекты; **S** – субъекты; {**R**} – множество видов доступа (операций) в сети (создание субъекта/объекта, обращение к ресурсу сервера базы данных, запрос на исходящее/входящее сообщения, удаление субъекта/объекта); {**T**} – множество требований к механизмам защиты АС (при передаче (шифрование, контроль целостности), при авторизации и аутентификации, при аудите и регистрации событий).

Для построения субъектно-объектной модели необходимо описать процесс взаимодействия между субъектами и объектами системы, управление информационными потоками в вычислительной среде.



Субъектно-объектная декомпозиция структуры АС

Обозначения сущностей и операций разработанной модели

Нами были выявлены сущности и операции, присущие и покрывающие архитектуру наиболее распространенных АС. Приведем единую таблицу формальных наименований операций, используемых для описания модели АС.

С помощью введенных формальных операций можно описать поведение АС в соответствии с разработанной политикой безопасности. При выполнении требований обеспечения информационной безопасности, предъявляемых к объектам и субъектам, а также к процедурам взаимодействия с ними, АС будет находиться в безопасном состоянии, в рамках выполнения описанного набора операций. В итоге использования модели удается сформулировать набор априорно неочевидных требований к компонентам сети и системе обеспечения безопасности. Совокупности этих требований должны отвечать компоненты сети и проектируемая система обеспечения безопасности.

Формальные наименования операций, используемых для описания модели АС

Обозначение	Наименование	Операнды	Выполняемая функция
$If(K_0 \mid A)$	Создание новой команды	Предыдущая команда, администратор	Если разрешено администратором, формируется новая команда
$\mathrm{Run}(O_i, K_0, S_i \mid A_0)$	Операция над объектом	Объект, команда, субъект, администратор	Если разрешено администратором, выполняется команда *Ко*
$[O_i, S_i] = Create(A_0)$	Создание пары субъект-объект	Объект, субъект, администратор	Создание пары субъект-объект
$O_i = Create(A_0)$	Создание объекта	Объект, администратор	Администратор создает объект
$A_j = Create(S_{A_i} \mid A_i)$	Создание администратора	Администратор, разрешение администратора	Создается администратор
$Delete(O_i, S_i \mid A_0)$	Удаление субъекта-объекта	Объект, субъект, администратор	Удаление пары субъект-объект
$Delete(A_i, S_i) \rightarrow A_m$	Удаление администратора	Администратор, разрешение администратора	Удаление администратора
$AddRights(S_A, K_0 \mid A) \rightarrow [O_i, S_i]$	Раздача прав	Администратор, команда, разрешение администратора	Пара субъект-объект наделяется правами доступа
$DelRights(S_A, K_0 \mid A) \rightarrow [O_i, S_i]$	Удаление прав	Администратор, команда, разрешение администратора	Удаление взаимных прав у пары субъект-объект
$AddAttribs(S_A, K_0 \mid A) \rightarrow S_i$	Присвоение атрибутов субъекту	Администратор, команда, разрешение администратора	Субъекту присваиваются атрибуты
$DelAttribs(S_A, K_0 \mid A) \rightarrow S_i$	Удаление атрибутов субъекта	Администратор, команда, разрешение администратора	У субъекта удаляются атрибуты

Список литературы

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1, 2, 3. – М.: ИПК Издательство стандартов, 2002.
2. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Москва, 2002.

Development of the Safety Information System Subject-Objective Model for the Automated System on its Decomposition Basis

S. N. Goncharov, A. V. Komarov, V. B. Medvedev

The subject-objective model describing conditions of automated system is submitted, allowing to divide safe and dangerous conditions, to formulate positions at which performance the system remain in a safe condition at realization of any transitions. Use of subject-objective model allows to formalize the description of a policy of safety and to construct is guaranteed the protected system.