УДК 004.056.53

ОБЕСПЕЧЕНИЕ МНОГОУРОВНЕВОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Даиров А.А.
Казахский национальный университет им. аль-Фараби, Алматы

Научный руководитель – Тунгатаров Н.Н.

Вопросы обеспечения безопасности информации играют важную роль в жизни общества, а в некоторых случаях и определяющую.

Для обеспечения информационной безопасности применяют комбинированные методы защиты, которые включают защиту информации от несанкционированного доступа средствами проверки полномочий пользователей и обслуживающего персонала на использование информационных ресурсов; идентификацию и аутентификацию сторон, производящих обмен информацией (подтверждение подлинности отправителя и получателя); разграничение прав пользователей и обслуживающего персонала при доступе к информационным ресурсам, а также при хранении и предоставлении информации с ограниченным доступом; распределение информации по степеням защищенности и по категориям доступа, сертификация технических и программных средств и другие методы.

Концепция надежной вычислительной базы является центральной при оценке степени гарантированности, с которой систему можно считать надежной. Надежная вычислительная база это совокупность защитных механизмов компьютерной системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности [1]. Основное назначение надежной вычислительной базы – выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами определенных операций (запросов) над объектами. Монитор обработки запросов (МОЗ) проверяет каждое обращение пользователя к программам или данным на предмет согласованности со списком действий, допустимых для пользователя. От МОЗ требуется выполнение трех свойств:

- изолированности, когда монитор защищен от отслеживания своей работы;
- полноты, когда монитор должен вызываться при каждом обращении и не должно быть способов его обхода;
- верифицируемости, когда монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Забота о возможности утечки информации возлагается на саму систему. Такие системы получили название систем многоуровневой защиты. Многоуровневая защита определяется как свойство вычислительной или информационной системы хранить и обрабатывать данные различного уровня и категорий пользования при наличии персонала с различными категориями допуска, таким образом, чтобы исключить доступ к информации или ее модификацию лицами, чей допуск не отвечает уровню секретности информации.

В зависимости от первоначального содержания информации, принадлежащей объекту, ему предписывается определенный уровень защиты. Уровни защиты приписываются также субъектам. Система защиты информации должна быть построена таким образом, чтобы в течение всего времени функционирования вычислительной системы ни один субъект не получил возможности доступа к информации, первоначально принадлежавшей объекту с более высоким или несравнимым уровнем защиты (по отношению к уровню защиты субъекта).

Математическая модель монитора обработки запросов подробно рассмотрена в [2, 3]. Рассмотрим применение математической модели МОЗ для разработки методики сертификации средств многоуровневой защиты.

Основными элементами математической модели являются: множество субъектов S; множество объектов *O)* множество уровней защиты L; множество видов доступа A; матрицы прав доступа M; список текущего доступа B; список запросов R.

Пусть множество субъектов *S* – конечное множество элементов s_1, s_2,..., s_m. Множество субъектов наделено структурой дерева: каждому субъекту s_jсоответствует список субъектов, непосредственно следующих за ним ("сыновей") и, если субъект $s_j \in S$ отличен от корня дерева s_k, ему соответствует единственный субъект $s_{g(j)}$, непосредственно предшествующий этому субъекту s_f, ("отец" субъекта s_j). Каждому субъекту s_j приписывается определенный уровень защиты $J(s_j), j \in J$, остающийся неизменным все время функционирования системы или все время существования субъекта вплоть до лишения его всех прав доступа к объектам системы.

Пусть множество объектов *O* - конечное множество o_1, o_2 , ... , o_n. Они пассивные носители информации. Примеры объектов: массивы информации (тексты), файлы данных, программы, подпрограммы и т.п., хранящиеся в оперативной памяти, на внешних носителях, в банках или базах данных и т.д. Каждый элемент (объект) имеет определенный уровень защиты $J(o_i)$, $i = \overline{1,n}$.

Если I - множество индексов {i / i=l, ... , n}, то для уровней защиты возможна запись: $J(o_i)$, $i \in I$. Этот уровень защиты объекта $J(o_i)$, постоянный для данного объекта $o_j \in O$, остается неизменным все время функционирования системы или все время существования объекта o_i, вплоть до его уничтожения. Поэтому назовем его базовым и обозначим $J_b(o_i)$. Наделим каждый объект o_i переменным (текущим) уровнем защиты $J_p(o_i)$ на тот случай, когда в процессе функционирования вычислительной системы объект o_i (программа, подпрограмма и т.п.) привлекается субъектом S_i в качестве своего подсубъекта.

Множество уровней защиты *L* - это конечное упорядоченное множество элементов $l_1, l_2, \ldots, l_k$: $l_1 > l_2 > \ldots > l_k$. Множество L изоморфно множеству категорий допуска, т.е. $\{l_i\} \xrightarrow{is} \{\mu_j\}$.

Множество видов доступа *A,* состоящее из следующих элементов (чтение, дополнение, запись, исполнение, отказ от доступа, передача прав, лишение прав, уничтожение, создание, запрос) например может быть определено как:

- вид доступа «чтение (Ч)» состоит в получении субъектом s_j информации, содержащейся в объекте o_i.
- вид доступа «отказ от доступа (О)» запрещает субъекту s_j доступ к информации объекта o_i. Отказ субъекта s_j от доступа к объекту o_i разрешается безусловно. В этом случае данный вид доступа $x \in A$ исключается из множества видов доступа субъекта.

Матрица прав доступа $M=||m_{ij}||$ – это прямоугольная матрица размерности m x n, каждый элемент m_{ij} которой содержит список видов доступа субъектов $s_j \in S$, $j = \overline{1,m}$, к объекту $o_i \in O$, $i = \overline{1,n}$, которые ему в данный момент разрешены и на которые он может претендовать.

Список текущего доступа *B* описывает разрешенный в данный доступ субъектов к объектам. Он содержит записи вида (s_j, o_i , x), если субъекту s_j, был разрешен доступ $x \in A$ к объекту o_i и это разрешение к настоящему моменту не отменено. Разрешение доступа действует до тех пор, пока субъект не обратиться с запросом об отказе от доступа к монитору обработки запросов.

Список запросов R содержит запросы всех видов доступа, содержащихся в множестве видов доступа: виды доступа субъектов к объектам, создания и уничтожения объектов, передачи и лишения прав доступа, а также отказ от доступа.

Разрешение запроса вызывает изменение состояния вычислительной системы для того, чтобы система защиты, использующая данный МОЗ, обеспечивала защиту, необходимую и достаточно. Это изменение должно приводить к защищенному состоянию, если исходное состояние также было защищено. Для этого необходимо строго выполнять решающие правила по разрешению запросов и изменению состояний [2].

Алгоритм сертификации монитора обработки запросов заключается в сравнении результатов доступа всех видов запросов всех субъектов ко всем объектам сертифицируемого МОЗ с результатами, полученные программным путем. При полном совпадении результатов считается, что сертифицируемый МОЗ соответствует заявленным параметрам. При несовпадении хотя бы одного результата считается, что сертифицируемые средства защиты не соответствуют заявленным параметрам.

Алгоритм включает следующие основные шаги:

- Ввод характеристик основных компонент монитора обработки запросов: ввод базы данных субъектов, ввод базы данных объектов, формирование данных матрицы доступа.
- Генерация запросов:

2.1 Выбирается субъект S_j ($j=\overline{1,m}$).

2.2 Генерируется запрос Z_k($k=\overline{1,9}$).

2.3 Выбирается объект o_i ($i=\overline{1,n}$).

2.4 Обращение к матрице доступа M(j,i)

2.5 Получение результата запроса.

2.6 Текущий запрос субъекта к текущему объекту обрабатывается сертифицируемым МОЗ.

2.7 Сравнение результаты запросов МОЗ с результатами, полученные в п. 2.5. При несовпадении считается, что МОЗ не прошел сертификацию и выход из программы.

2.8 Переход к 2.3, пока не все объекты исчерпаны.

2.9 Переход к 2.2 на выбор следующего запроса, пока не все виды запросов обработаны.

2.10 Переход к 2.1 на выбор следующего субъекта, пока все субъекты не будут исчерпаны.

2.11 Конец работы.

Каждая запись базы данных субъектов описывает субъект по следующей структуре: шифр субъекта, имя субъекта, указатель на отца субъекта, классификация субъекта, код доступа субъекта. Структура этой базы такова, что она описывает дерево, где каждый субъект имеет указатель на «отца», если он не главный субъект. Главный субъект является корнем дерева и не имеет указателя.

Каждая запись базы данных объектов описывает объект, созданный субъектом и имеет следующую структуру: имя объекта, шифр субъекта создателя, шифр объекта, классификация субъекта создателя, код доступа объекта.

Каждая запись БД матрицы прав доступа имеет следующую структуру: имя субъекта, имя объекта, список видов доступа субъекта к объекту.

Доступ к информации организован таким образом, что каждый субъект имеет право обратиться к объекту только с тем видом доступа, который имеется в списке.

Разработанное программное средство разграничения доступа с применением условий Белла-ЛаПадула может быть применено для систем управления государственными органами с древовидной структурой субъектов и объектов защиты информации.

Литература

1. Д.П.Зегжда, А.М. Ивашко. Основы безопасности информационных систем. - М.: Горячая линия - Телеком , 2000.

2. Bell D.E., La Padula L.J. Secure computer system: mathematical foundations. MTR - 2547, vol.1, MITRE Corp., March 1973.
3. Bell D.E., La Padula L.J. Secure computer system: mathematical foundations. MTR - 2547, vol.11, MITRE Corp., March 1973.