УДК 598.87

АНАЛИЗ МОДЕЛЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Голубева А.К., Куржеевский И.В., Филимонова А.В.

Академия военно-морских сил имени П.С.Нахимова, Украина

Аннотация

Приведен сравнительный анализ основных моделей безопасности информационных систем. На основе анализа сделан вывод о необходимости включения в модели безопасности систем принятия решений по защите информации в условиях неопределенности на основе математического аппарата нечетких множеств.

Was done the comparative analysis of the main models of safety of information systems. On the basis of the analysis is drawn the conclusion that need inclusion for model of safety - systems of decision-making on protection of information in the conditions of uncertainty on the basis of mathematical apparatus of indistinct sets.

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 обходиться 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. Основную роль в методе формальной разработки системы играет так называемая модель безопасности (модель управления доступом, модель политики безопасности). Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации. Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

Модели безопасности

Назначение моделей безопасности состоит в том, что они позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры и используемые при ее построении технологические решения. Среди моделей политики безопасности можно выделить два основных типа:

1 дискреционные (произвольные);
2 мандатные (нормативные).

В основе этих моделей лежат, соответственно, дискреционное управление доступом (Discretionary Access Control - DAC) и мандатное управление доступом (Mandatory Access Control - MAC).

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. К недостаткам относится статичность модели (данная политика безопасности не учитывает динамику изменений состояния АС, не накладывает ограничений на состояния системы. В качестве классических примеров моделей этих типов можно назвать дискреционную модель Харрисона-Руззо-Ульмана (модель HRU) и мандатную модель Белла-Лападула (модель БЛ). Однако существует также и ролевая модель, которая очень близка к дискреционной, но при этом содержит признаки мандатной модели доступа.

Первой моделью системы безопасности стала модель Белла - Ла-Падулы (Bell-LaPadula model), созданная в 1973-74 годах в MITRE в городе Белфорде в штате Массачусетс по заказу Военно-Воздушных сил США. В 76 году была дополнена до использования в пределах концепции MULTICS (информационно-вычислительная система с мультиплексированием каналов передачи данных), в 86 году адаптирована для использования в сетевых системах. В изначальном варианте модель Белла – Ла-Падулы предусматривала возможность только мандатный контроль за доступом. В целом модель Белла - Ла-Падулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено.

Недостатки модели состоят в том, что

- основная теорема является избыточной по отношению к определению безопасного состояния. т.к. ограничения, накладываемые теоремой на функцию перехода, совпадают с критерием безопасности состояния;
- из теоремы следует только то, что все состояния, достижимые из безопасного состояния при определенных ограничениях, будут в некотором смысле безопасными, но при этом не гарантируется, что процесс осуществления перехода будет безопасным.

Еще из недостатков модели стоит отметить невозможность передачи информации от более высокого уровня к нижним, поскольку это значительно снижает возможности управления субъектами. В рамках модели возможно создание незащищенных систем.

Дискреционная модель Харрисона-Руззо-Ульмана реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

Положительные моменты:

- данная модель является простой в реализации (т.к. не требует применения сложных алгоритмов);
- данная модель является эффективной в управлении (т.к. позволяет управлять полномочиями пользователей с точностью до операции над объектом);
- критерий безопасности данной модели является весьма сильным в практическом плане (т.к. позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия).

Отрицательные моменты:

- доказано, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния Q0 (S0, O0,M0) и общего правила r решить, является ли данная информация безопасной;
- существует уязвимость к атаке с помощью «троянского коня» (т.к. в дискреционных моделях контролируются только операции доступа субъектов к объектам, а не потоки информации между ними).

В условиях информационного противоборства, администратор системы защиты информации, принимающий решения по управлению защитой на основе модели безопасности, не обладает полной информацией обо всех факторах, учет которых влияет на это решение. Основой информационного противоборства является информированность конфликтующих сторон о действиях друг друга. Каждая из противоборствующих сторон обладает определенной информационной средой. Под информационной средой нападения или защиты будем понимать общее количество информации, которой обладает та или иная сторона конфликта, но в большинстве случаев это количество информации неизвестно. Поэтому, приходится принимать решения в условиях неопределенности. Следовательно, по мнению авторов необходимо дополнить модели безопасности системами принятия решений по защите информации в условиях неопределенности, на основе использования математического аппарата нечетких множеств, что является направлением дальнейшего исследования.

Выводы

Общая теория моделей политики безопасности подразумевает выполнение всех требований, но существующие реализации теории ориентированы на выполнение только их части в полном объеме, что подразумевает значительное ограничение на возможные области каждой модели. С течением времени это тенденция усиливается, и в настоящее время модели фактически разрабатываются специально под определенные реализации, что в целом не уменьшает их ценности в практическом плане. Стоит заметить, что, как и большинство технологий безопасности, модели политики безопасности все больше переходят из области военных разработок в область коммерческого и общего использования, что в значительной мере связано с развитием сетевых технологий.

Список использованных источников:

1. Девянин П.Н. Модели безопасности компьютерных систем. Издательский центр «Академия», 2005. 143 с.
2. Гаценко О.Ю. Защита информации. Основы организационного управления. СПб.:Изд.дом «Сентябрь», 2001. 228 с.