П. Н. Лось

ПОСТРОЕНИЕ МОДЕЛИ БАЗЫ ЗНАНИЙ ДЛЯ ЭКСПЕРТНОЙ СИСТЕМЫ АУДИТА БЕЗОПАСНОСТИ

В этом документе рассматривается проблема описания и проектирования базы знаний(БЗ) для экспертной системы(ЭС) аудита компьютерной безопасности.

Введение

Построение модели интеллектуального анализа компьютерной безопасности является частью масштабного процесса, в который входят все задачи, от формулировки вопросов выбора и хранения данных и создания модели до развертывания модели в рабочей среде. В этом документе показаны особенностей построения модели анализа компьютерной безопасности.

I. Проектирование базы знаний для ЭС

Целью базы знаний экспертной системы является представление специфичных для предметной области знаний в форме, которую компьютер может использовать для эффективной работы с этими знаниями.

Структура проектируемой системы показана на рисунке 1. База знаний для анализа представляет собой набор фактов, которые отражают состояние компьютерной системы, информация об уязвимостях программного обеспечения и возможные сетевые проблемы. Правила взаимодействия (Interaction rools) определяют, как различные части системы могут взаимодействовать и влиять на безопасность. Interaction rools определяют семантику ЭС: различные виды уязвимостей и способы их возникновения, поведение программного обеспечения, влияющее на безопасность, конфигурация доступа к сети. Политика безопасности (Security policy) - это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности. В разрабатываемой системе политика - это кортежи, которые перечисляют права доступа к данным для пользователей.

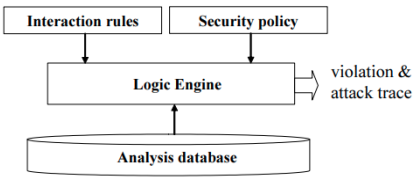

Рис. 1 – Структура ЭС

Онтология состоит из 4 основных сущностей и отношений между ними:

1. Модель аппаратного домена. Является абстракцией для описания проверяемой машины и всей информации о сети, к которой подключена эта машина.

2. Модель активов (Assets) - это активы, наиболее ценные ресурсы в системе. В качестве актива могут выступать различные источники данных: база данных, файл или системная служба. Иногда определение актива может быть расплывчатым, но, как правило, это все, что важно для организации-владельца или пользователя.

3. Модель программного обеспечения. Описывает существующее(установленное) ПО на данной машине. Программное обеспечение может зависеть от другого программного обеспечения и, следовательно, любая часть программного обеспечения, которая зависит, например, от неисправной библиотеки, также потенциально уязвима.

4. Модель безопасности пользователя. Описание пользователей, рабочих групп.

II. Выводы

Описание модели предметной области было выполнено, не привязываясь к определенной реализации или операционной системе. При этом описание является достаточным, что бы идентифицировать каждую сущность, ее связи и поведение в системе.

Лось Павел Николаевич, магистрант кафедры интеллектуальных информационных технологий БГУИР pasha-los96@yandex.ru.

Научный руководитель: Захаров Владимир Владимирович, доцент кафедры интеллектуальных информационных технологий БГУИР, кандидат технических наук, доцент, zvv@open.by.