Применение экспертных систем для решения задач информационной безопасности

ТАТУ СФ асс.Иброхимова З.Э.

Возможностъиспользования экспертных систем для решения задач защиты информации стала интересоватъ специалистов по информационной безопасности в связи с бурным развитием информационных технологий, а, следователъно, и появлением новых видов угроз. Уже сейчас экспертные системы применяются для решения некоторых задач информационной безопасности:

- оценка рисков и составление модели угроз;
- антивирусное программное обеспечение;
- аудит информационной безопасности предприятия;

Несмотря на все многообразие решаемых задач, можно выделить два основных подхода к созданию экспертных систем:

- создание экспертных систем, использующих эвристические правила;
- создание самообучающихся экспертных систем;

Экспертные системы на основе эвристических правил.

В данном подходе используется один из популярных методов представления знаний - правила в форме IF<условие>THEN<action>. Одним из применений такого подходя является создание антивирусного программного обеспечения и систем обнаружения вторжений. Возможны следующие варианты эвристического анализа:

- Анализируется программный код файла и сравнивается с сигнатурами, хранящимися в базе антивирусного ПО. Эти сигнатуры характеризуют не какой-либо конкретный вид вредоносного ПО, а некоторую совокупность вирусов, исходя из предположения о том, что новые вирусы имеют сходство с уже существующим вредоносным ПО;
- Анализируются действия, совершаемые рассматриваемым процессом во время работы, и сравниваются с правилами, сохраненными в базе антивирусного ПО. В этом случае появляется возможность обнаружить

вредоносное ПО, сигнатуры для которого еще не были добавлены в базу, если оно нацелено на выполнение тех же действий, что и ранее встречавшиеся вирусы.

Примерами антивирусного ПО, использующего эвристический анализ, могут послужить ESETThreatSenseKaspersky, Dr.WebKatana.

Кроме того, эвристические механизмы могут также использоваться с целью автоматизации аудита информационной безопасности. К примеру, система контроля защищенности и соответствия стандартам MaxPatrol, разработанная компанией PositiveTechnologies, использует эвристический анализ для выявления уязвимостей в сетевых службах и приложениях, давая оценку защищенности сети со стороны злоумышленника.

Данный подход к созданию экспертных систем обеспечивает простоту программирования и представления данных, так как знания, использующиеся в разрабатываемых системах, могут быть представлены в сравнительно простой форме эвристического правила. Кроме того, системы на основе эвристических правил могут быть разработаны без использования специальных средств (таких, как среда программирования CLIPS, язык логического программирования PROLOG). К недостаткам подобных систем можно отнести необходимость постоянного обновления баз знаний и полиномиальное возрастание числа ложных срабатываний создающихся систем при чрезмерной чувствительности эвристического анализатора.

Семантические сети

Другой подход, применимый для решения задач информационной безопасности - использование семантических сетей. С точки зрения математики данная структура представляет собой помеченный ориентированный граф, узлы которого представляют объекты, а дуги - связи между этими объектами.

Подобный способ представления знаний может быть использован для описания многих предметных областей, в том числе и относящихся к сфере информационной безопасности. Пример использования семантических сетей

для представления знаний в области защиты информации представлен в работе. В данной работе представлено построение модели данных о различных уязвимостях на основе онтологического подхода, которая затем может быть использована для моделирования сетевых атак.

Рассмотрим достоинства и недостатки семантических сетей как способа представления знаний в экспертных системах. К достоинствам можно отнести следующие моменты:

- с помощью выбора соответствующих связей между объектами в семантической сети, становится возможной описание сколь угодно сложной предметной области.
- представленная графически, система знаний является более наглядной;

Но данный подход также имеет и некоторые недостатки:

- сетевая модель не содержит ясного представления о структуре предметной области;
- подобные модели являются пассивными структурами, а потому требуют специальный аппарат формального вывода для обработки;
- при осуществлении поиска узлов возникает комбинаторный взрыв, особенно если ответ на запрос является отрицательным.

Комбинирование подходов.

Каждый из описанных выше подходов обладает собственными преимуществами и недостатками. Тем не менее, представляется возможным комбинирование этих подходов с целью упорядочения эвристических правил и ускорения классификации атаки или вредоносного программного обеспечения.

В данной модели предполагается следующая структура: в узлах графа, представляющего семантическую сеть, находятся эвристические правила, позволяющие отнести атаку либо вредоносное программное обеспечение к тому или иному типу/классу. Дуги же в этой модели будут представлять отношения, показывающие связь между различными правилами. Сами правила должны располагаться на нескольких уровнях, причем каждый

последующий уровень должен определять более узкий класс угроз (рис. 1).

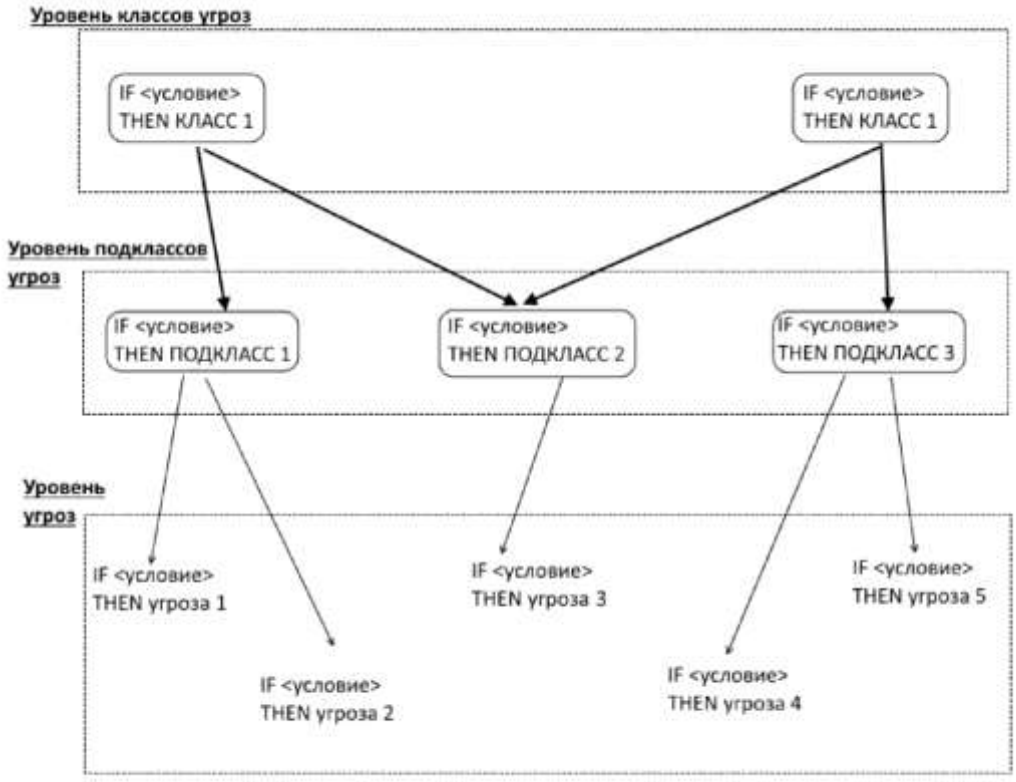

Рис. 1 - Представление модели данных в виде графа

Таким образом, построив подобную семантическую сеть, содержащую в своих узлах эвристические правила для классификации класса атак или угроз, предполагается получить увеличение скорости определения типа угрозы, а, следовательно, увеличение производительности системы обнаружения вторжений.

Литература

1. *Лепехин А. Н.* Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с. — ISBN 978-985-463-258-2.
2. *Малюк А. А.* Теория защиты информации. — М.:Горячая линия — Телеком, 2012. — 184 с. — ISBN 978-5-9912-0246-6.
3. *Родичев Ю.* Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.

4. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
5. *Петренко С. А.* Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
6. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с. — ISBN 5-94074-383-8.