УДК 007.3

С.А. Козлова – магистрант

ФГБОУ ВО Пермский ГАТУ, г. Пермь, Россия

ПРИМЕНЕНИЕ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С развитием Интернет-технологий многие компании, специализирующиеся в сфере информационных технологий, ежегодно вкладывают огромные средства в создание соответствующего инструментария интеллектуальной обработки текстовой, речевой и графической информации. В связи с развитием технологий специалистов по информационной безопасности стала интересовать Возможность использования экспертных систем для решения задач защиты информации. В следствии развития технологий появились новые виды угроз. Уже сейчас экспертные системы применяются для решения некоторых задач информационной безопасности таких как [1]:

* 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 подхода 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 программного обеспечения. Эти сигнатуры характеризуют не какой-либо конкретный вид вредоносного программного обеспечения, а некоторую совокупность вирусов, исходя из предположения о том, что новые вирусы имеют сходство с уже существующим вредоносным программного обеспечения;

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.

Эвристические механизмы могут также использоваться с целью автоматизации аудита информационной безопасности. К примеру, система контроля защищенности и соответствия стандартам MaxPatrol, разработанная компанией Positive Technologies, использует эвристический анализ для выявления уязвимостей в сетевых службах и приложениях, давая оценку защищенности сети со стороны злоумышленника [2].

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. Системы на основе эвристических правил могут быть разработаны без использования специальных средств. К недостаткам подобных систем можно отнести необходимость постоянного обновления баз знаний и полиномиальное возрастание числа ложных срабатываний создающихся систем при чрезмерной чувствительности эвристического анализатора.

Другой подход, применимый для решения задач информационной безопасности – использование семантических сетей. Подобный способ представления знаний может быть использован для описания многих предметных областей, в том числе и относящихся к сфере информационной безопасности [3]. Можно выделить несколько достоинств семантической сети, а именно с помощью выбора соответствующих связей между объектами в семантической сети, становится возможной описание сколь угодно сложной предметной области и представленная графически, система знаний является более наглядной. Недостатки у данной семантической сети тоже есть [4]:

* 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

Выше описанные подходы обладают собственными преимуществами и недостатками. Совмещение этих подходов возможно 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 (рисунок 1).

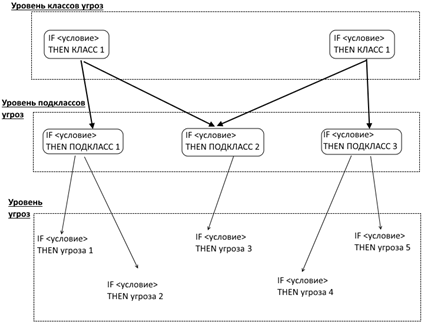


Рисунок 1-Представление модели данных в виде графа

Построив подобную семантическую сеть, содержащую в своих узлах эвристические правила для классификации класса атак или угроз, предполагается получить увеличение производительности системы при обнаружении вторжений.

Рассмотрев подходы к использованию экспертных систем для решения задач информационной безопасности, были предложены несколько вариантов. Компании для защиты информации могут выбрать для себя наиболее подходящий вариант подхода.

Литература

1. Плетнёв П.В. Алгебраический подход к оценке информационной безопасности / Плетнёв П.В., Лёвкин И.В. // Известия Алтайского государственного университета. №1-2. C. 124-127
2. MAXPATROL COMPLIANCE AND VULNERABILITY MANAGEMENT SYSTEM [Электронный ресурс] URL: https://goo.gl/l0gNIc
3. Котенко И.В. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода / Котенко И.В., Полубелова О.В., Чечулин А.А. // Труды СПИИРАН. 2013. Вып. 26. C. 26-39.
4. Башмаков А.И., Башмаков И.А. Интеллектуальные информационные технологии: Учеб. пособие. – М.: МГТУ им. Н.Э. Баумана, 2005. – 304 с.