Оценка угроз информационной безопасности методами алгебры логики

В данной работе приводится описание процесса оценки угроз информационной безопасности, а также рассматривается способ применения когнитивно-ориентированных моделей и схем вывода, в частности таких средств, как Сорит и семантические сети, для оценки угроз ИБ.

Основная идея предполагаемого подхода определения угроз ИБ состоит в следующем. На бае вопросников, заполняемых в ходе аудита, формируют унарные и бинарные высказывания, после чего строят Сорит, результатом которого являются факты, влекущие за собой угрозы ИБ [Козлов Л.А. Когнитивное моделирование на ранних стадиях проектной деятельности. Барнаул:Изд-во АлтГТУ,2009]. Затем на основании исчисления предикатов строят модель актуальных угроз,а именно угроз, влекущих утечку информации. Таким образом, используя данные процедуры, формируют семантическую сеть,с итогом использования на большом количестве предметных областей. Результатом построения такой сети является формирование базы знаний, позволяющей определять угрозы информационной сети, имея на входе лишь ее формальное описание. Ниже приведем каждого этапа более подробно.

Для построение Сорита необходим ряд исходных унарных высказываний. В примере рассмотрим исходные высказывания, касающиеся использования на предприятии отчуждаемых носителей информации.

1)W0 — рассматриваемая организация;

2)W1 — организация,,в которой используют гибкие магнитные диски (ГМД);

3)W2 — организация, имеющая уязвимое звено «отчуждаемые носители информации»

4)W3 — организация, подверженная угрозе хищения носителей;

5)W4 — организация подверженная угрозе уничтожения носителя;

6)W5 — организация, подверженная угрозе потере утери носителя.

На основе унарных высказываний сформируем бинарные высказывания, в которых задействованы традиционные для формальной логики кванторы:

A,W0,W1 – рассматриваемая организация есть организация,в которой используют гибкие магнитные диски (ГМД)

Данное бинарное высказывание строим, исходя из фактической ситуации на предприятии. Далее перечислены бинарные высказывания, справедливые для любой организации.

A,W1,W2 — высокая организация, в которой используют ГМД,есть организация, имеющая уязвимое звено «отчуждаемые носители информации».

A,W2,W4 — организация, имеющая уязвимое звено «отчуждаемые носители информации», подверженная угрозе хищения носителей.

A,W2,W5 — организация , имеющая уязвимое звено «отчуждаемые носители информации», есть организация, подверженная угрозе уничтожения носителей.

- организация, имеющая уязвимое звено «отчуждаемые носители информации»,есть организация,подверженная угрозе утери носителей.

Бинарные высказывания с точки зрения силлогистики Аристотеля, представляют собой одну из посылок силлогизма соответствующим квантом A E I O. Эти посылки могут сочетаться в различных комбинациях друг с другом. Результате чего будут получены новые заключения. Заключения также можно сочетать между собой до тех пор, пока естественный переход от сильных модусов к слабым не остановит процесс порождения новых выводов [Поспелов Д.А. Моделирование рассуждений. Опыт анализа мыслительных процессов. М.:Радио и связь, 1989.].

Сорит, построенный на основе исходных посылок, представлен на рис.1. В результате построения сорита получены следующие выводы:

1) A,W0,W3 — рассматриваемая организация есть организация, подверженная угрозе хищения носителей;

2)A,W0,W4 — рассматриваемая организация есть организация, подверженная угрозе уничтожения носителей;

3)A,W0,W5 — рассматриваемая организация есть организация, подверженная угрозе потери носителей;

Данный метод применяется в разработанной онлайн-системе «SAFE-DOC.com».

Пользователь в личном кабинете вносит информацию о составе компьютерной техники, серверах, а так же работниках, допущенных до обработки конфиденциальной информации. Следующим этапом пользователь должен описать характеристики используемых информационных систем, обрабатывающих конфиденциальную информацию. На основе введенных данных формируется уровень защищенности информационной системы и формируется типовая модель угроз для данной системы. Пользователь, при необходимости, убирает/добавляет актуальные угрозы информационной системы.

На основании полученных данных о рабочих местах, информационных системах, уровнях защищенности и актуальных угроз онлайн-сервис «SAFE-DOC.com» автоматически подбирает необходимый состав средств защиты информации, и выдает три варианта спецификации, состоящих из идентичных средств защиты информации, но разных производителей.

Пример выполнения последовательности проведения оценки угроз информационной безопасности для информационных систем персональных данных (далее – ИСПДн) в онлайн-системе «SAFE-DOC.com»:

Шаг 1 Описание информационной системы персональных данных

В описании приводятся:

− цель функционирования информационной системы персональных данных, параметры, определенные при установлении уровня защищенности, перечень обрабатываемых данных, их объем;

− территориальное расположение информационной системы персональных данных относительно границ контролируемой зоны;

− состав и характеристики технических и программных средств информационной системы персональных данных.

Шаг 2 Определение пользователей информационной системы персональных данных

Все пользователи информационной системы персональных данных имеют собственные роли. Необходимо представить список типовых ролей.

Шаг 3 Определение исходного уровня защищенности

Уровень исходной защищенности определяется по таблице 1 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 14.02.2008.

Шаг 4 Определение вероятности реализации угроз в информационной системе персональных данных

Данный параметр определяется экспертным путем, исходя из предположений о возможностях нарушителей, каналах и способах реализации угроз.

Шаг 5 Определение возможности реализации угроз в информационной системе персональных данных

Определяется в соответствии с «Методикой определения актуальных УБПДн при их обработке в ИСПДн» ФСТЭК России.

Шаг 6 Оценка опасности угроз

Оценивается экспертным путем в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 14.02.2008.

Шаг 7 Определение актуальности угроз в ИСПДн

Определяется в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 14.02.2008.

Шаг 8 Определяется перечень актуальных угроз путем выбора актуальных из перечня всех угроз

Шаг 9 Документально оформляется и утверждается частная модель угроз

Шаг 10 Документально оформляется и утверждается спецификация необходимых средств защиты информации.