УДК 681.3.067

П.В. Плетнёв, И.В. Лёвкин

Алгебраический подход к оценке информационной безопасности

P.V. Pletnev, I.V. Levkin

The Algebraic Approach to the Estimation of Information Safety

В данной статье приводится описание процесса оценки рисков информационной безопасности, а также рассматриваются способы применения когнитивно-ориентированных моделей и схем вывода, в частности таких средств, как сорит и семантические сети для оценки рисков информационной безопасности.

Ключевые слова: информационная безопасность, оценка угроз, оценка рисков, моделирование.

The given article describes a process of the estimation of informational safety risks, and also considers ways to apply the cognitively oriented models and output circuits, in particular such resources as litters and semantic nets for estimation of informational safety risks.

Key words: information safety, threat estimation, risk estimation, modeling.

Основная идея определения угроз информационной безопасности состоит в том, что на основе информации, собираемой в ходе аудита безопасности информационной системы (ИС), формируются унарные и бинарные высказывания, на основании которых строятся логические выводы, результатом которых являются факты, влекущие за собой угрозы информационной безопасности. Затем при помощи исчисления предикатов формируется модель актуальных угроз, влекущих утечку информации. Таким образом, формируется семантическая сеть, на основании которой формируется база знаний, позволяющая идентифицировать угрозы и риски в информационной сети по ее формальному описанию.

Опишем процесс оценки рисков информационной безопасности и рассмотрим способ применения когнитивно-ориентированных моделей и схем вывода, в частности, таких средств, как логический вывод и семантические сети.

Для построения логического вывода необходим ряд исходных унарных высказываний. Рассмотрим пример угроз использования на предприятии отчуждаемых носителей информации:

1. W0 – рассматриваемая организация.
2. W1 – организация, в которой используются гибкие магнитные диски (ГМД).
3. W2 – организация, имеющая уязвимое звено «отчуждаемые носители информации».
4. W3 – организация, подверженная угрозе хищения носителя.
5. W4 – организация, подверженная угрозе уничтожения носителя.
6. W5 – организация, подверженная угрозе утери носителя.

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

1. *A, W0, W1* – рассматриваемая организация есть организация, в которой используются гибкие магнитные диски (ГМД). Данное бинарное высказывание строится исходя из фактической ситуации на предприятии. Далее перечислены бинарные высказывания, справедливые для любой организации.
2. *A, W1, W2* – всякая организация, в которой используются ГМД, есть организация, имеющая уязвимое звено «отчуждаемые носители информации».
3. *A, W2, W3* – организация, имеющая уязвимое звено «отчуждаемые носители информации», подвержена угрозе хищения носителя.
4. *A, W2, W4* – организация, имеющая уязвимое звено «отчуждаемые носители информации», подвержена угрозе уничтожения носителя.
5. *A, W2, W5* – организация, имеющая уязвимое звено «отчуждаемые носители информации», подвержена угрозе утери носителя.

С точки зрения силлогистики Аристотеля [1, 2], бинарные высказывания являются одной из посылок силлогизма с соответствующим квантором *A, E, I* и *O*. За счет их взаимных сочетаний могут быть получены новые заключения, которые также можно сочетать между собой до тех пор, пока естественный переход от сильных модусов к слабым не остановит процесс порождения новых выводов.

Логический вывод, построенный на основе исходных посылок, представлен на рисунке 1. В результате его построения получены следующие выводы:

A, W0, W3 – рассматриваемая организация есть организация, подверженная угрозе хищения носителя;

A, W0, W4 – рассматриваемая организация подвержена угрозе уничтожения носителя;

A, W0, W5 – рассматриваемая организация подвержена угрозе утери носителя.

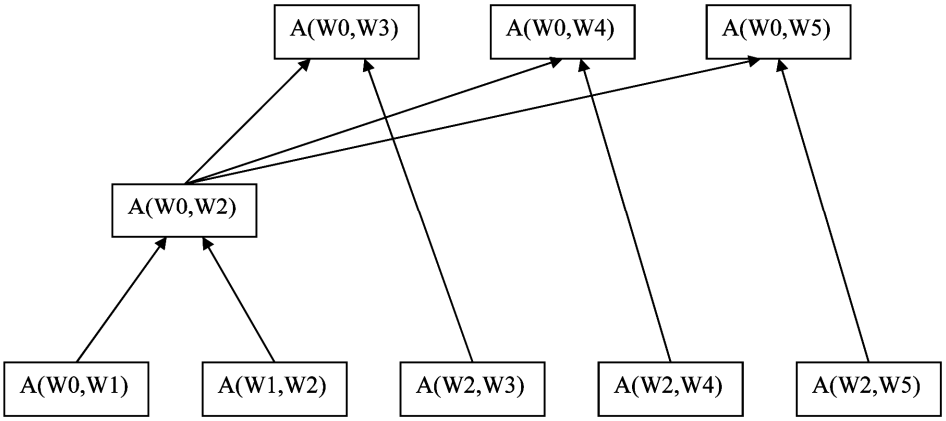

Рис. 1. Пример результата логического вывода

В результате получаем возможные факты утечки информации.

Перейдем ко второму этапу – определению актуальности угроз.

Изначально должно быть задано пять множеств и три предиката.

Множества:

• X – множество фактов (например, сервер установлен в отдельном помещении, кабели проложены в специальных коробах и т.д.);

• Y – множество уязвимостей (уязвимых звеньев);

• Z – множество угроз безопасности информации;

• Q – множество вопросов, задаваемых пользователю для определения актуальности угроз;

• W – множество ответов.

Предикаты:

• $P1(x,y)$ – предикат, определенный на X и Y и задающий отношение «если на предприятии имеет место факт x, $x \in X$, то имеется и уязвимость y»;

• $P2(y,z)$ – предикат, определенный на множествах значений Y и Z и задающий отношение «если на предприятии имеется уязвимость y, то имеется и угроза безопасности z»;

• $P3(q,w)$ – предикат, определенный на множествах значений Q и W и задающий отношение «отчетом на вопрос q, является ответ w».

На основании исходных данных о предприятии выбирается некоторое подмножество $X1 \subseteq X$. С помощью предиката $P1$ определяется подмножество $Y1 \subseteq Y$ – множество уязвимостей предприятия. С помощью предиката $P2$ определяется подмножество $Z1 \subseteq Z$ – множество угроз безопасности информации на предприятии.

Пользователь, отвечая на вопросы, определяет значения предиката P3 для всего множества значений Q и W. Каждому значению множества W соответствует некоторая вероятность. Далее с помощью предиката $P3$ заполняется матрица $P'' = |Pij|$, $i = 1,2,\ldots, n$; $j = 1,2,\ldots m$, где Pij – вероятность того, что могут сложиться благоприятные условия для использования j-ой уязвимости для реализации i-ой угрозы.

Вероятность наличия благоприятных условий для реализации j-ой угрозы определяется согласно формуле:

$$P^*_j = 1 - \prod_{k=1}^{k} (1 - p''_{jk}).$$

Таким образом, с помощью количественной оценки вероятности реализации угрозы можно осуществить качественную интерпретацию. Для получения комплексной оценки актуальности угрозы необходимо ввести данные о величине ущерба [3, 4]. Угроза признается актуальной, если показатель ее актуальности, представленный в вербальной интерпретации, попадает в область, обозначенную на рисунке 2.

		Вероятность реализации угрозы				
		Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Коэффициент опасности угрозы	Очень низкий					
	Низкий					
	Средний					
	Высокий					
	Очень высокий					

Рис. 2. Значения показателя актуальности угрозы, при которых она признается актуальной

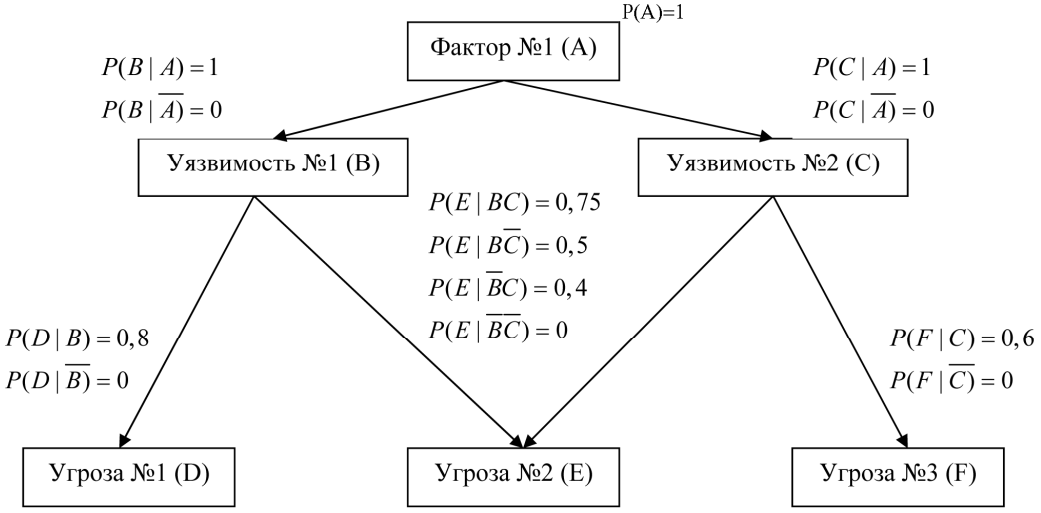

Рис. 3. Пример байесовской сети доверия

Рассмотренная предикативная модель может быть представлена в виде байесовской сети доверия, которая представлена на рисунке 3.

Байесовская сеть доверия – вероятностная модель, представляющая собой множество переменных и их вероятностных зависимостей. Формально это направленный ациклический граф, вершины которого представляют переменные, а ребра – условные зависимости между переменными [5].

Для нахождения безусловной вероятности события должны быть заданы условные вероятности всех *2n* событий, от которых оно зависит при наличии n предков.

Этот метод применяется, для того чтобы сократить оценку *2n* вероятностей, которые необходимы при использовании таблиц условных вероятностей. Согласно ему, вероятность события *y* в зависимости от набора вершин *Xr* оценивается по следующей формуле:

$$p(y \mid x_1, x_2 ... x_n) = 1 - \prod_{i=1}^{n} (1 - p(y \mid x_i)).$$

Как видно, она полностью соответствует формуле для предикативной модели.

Выборка (построение сорита) и оценка актуальных угроз утечки информации (исчисление придекатов) позволяют унифицировать данный процесс при помощи разработанного программного продукта – «Определитель вероятности реализации угрозы», который представляет собой совокупность двух модулей:

– модуль первичного сбора данных и расчета вероятностей реализации угроз безопасности информации;

– модуль редактирования данных о вопросах, уязвимостях, угрозах и связей между ними.

В аудиторской деятельности ООО «Центр информационной безопасности» сформирована значительная база знаний, которая анализируется при помощи использования семантических сетей по следующей схеме.

Семантическая сеть разбивается на составные части для упрощения вычисления, каждую из которых можно представить как выражение алгебры логики. Вычисление выражений производится при помощи упрощения, использования правил вывода, представленных далее. Результатом анализа является вывод об актуальности или неактуальности рассматриваемой угрозы.

Семантическая сеть – эффективный инструмент отображения информации и анализа. На ней в графическом виде показаны объекты и связи между ними. С помощью этой модели реализуются такие свойства системы знаний, как интерпретируемость и связность. За счет этих свойств семантическая сеть позволяет снизить объем хранимых данных, обеспечивает вывод умозаключений по ассоциативным связям, облегчает доступ к знаниям – начиная движение от некоторого понятия, по дугам отношений можно достичь других понятий, – восприятие аналитической информации, экономит время на ее понимание и принятие решений.

Преимущество данного метода анализа в том, что наиболее логически структурированные связи между объектами, база знаний занимают меньший объем, так как не используют такой побочной информации, как вес вершин, функций обработки. Операторы алгебры логики позволяют наиболее быстро анализировать знания, в отличие от расчетов функций второго метода.

Описанный в данной статье концептуально новый подход к определению угроз информационной безопасности позволяет уйти от экспертного анализа информационных систем, снизить риски ошибок по причине человеческого фактора, а главное – алгоритмизировать и унифицировать подход к определению угроз утечки информации как одного из главных моментов в защите информационных систем предприятий и организаций.

Библиографический список

1. Козлов Л.А. Когнитивное моделирование на ранних стадиях проектной деятельности. – Барнаул, 2009.

2. Поспелов Д.А. Моделирование рассуждений. Опыт анализа мыслительных процессов. – М., 1989.

3. Петренко С.А., Симонов С.В. Управление информационными рисками // Экономически оправданная безопасность. – М., 2004.

4. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная заместителем директора ФСТЭК 18 мая 2007 г.

5. Завгородний В.И. Системный анализ информационных рисков предприятия // Вестник Финансовой академии. – 2008. – №4.