М. В. Тимонин, В. С. Лаврентьев

ПРИМЕР МОДЕЛИРОВАНИЯ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ТЕОРИИ НЕЧЕТКОЙ МЕРЫ

В опубликованной ранее статье [1] был предложен подход к моделированию риска информационной безопасности с помощью теории нечеткой меры. Рассмотрим практический пример для наглядной демонстрации данной методики.

Построение модели информационной системы, позволяющей провести оценку риска информационной безопасности, включает следующие этапы:

1. Определение информационных активов;
2. Определение информационной структуры — расположения активов, связей и процессов;
3. Определение возможных путей атаки. Построение дерева атак;
4. Связь критериев оценки с элементами дерева атаки;
5. Приоритизация критериев и групп критериев. Выявление достаточных и необходимых условий, расстановка весов;
6. Проведение оценки информационной системы на основе определенных в п. 4 критериев;
7. Агрегация значений индивидуальных критериев с помощью интеграла Шоке;
8. Расчет общего значения риска.

Рассмотрим построение модели на примере (Рис. 1). Предположим, оценивается риск, связанный с потерей конфиденциальности информации из базы данных. Эта информация является активом. Второй шаг — описание инфраструктуры для определения месторасположения актива в ней и выявления потенциальных путей атаки.

База данных располагается на удаленной площадке Site 1, соединенной с офисом каналом Chanel 1. На этой же площадке находится ленточная библиотека Tape Library, содержащая ежедневные резервные копии базы данных. Кроме того, существует онлайн-копия базы, располагающаяся на площадке Site 2, соединенной с площадкой Site 1 каналом Chanel 2, а с офисом — каналом Chanel 3. Пользователи БД находятся в офисе.

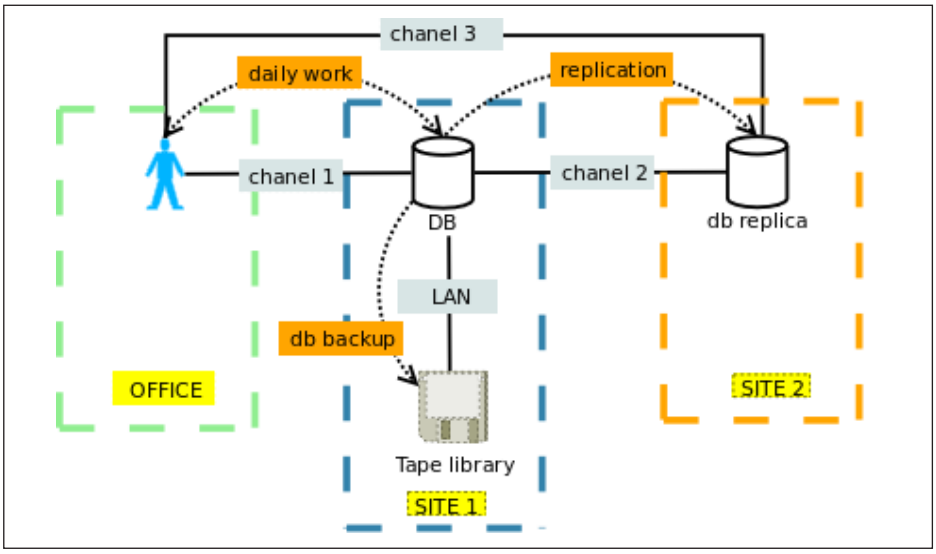

Рис. 1. Пример инфраструктуры организации

После построения данной диаграммы становится возможным определение потенциальных сценариев атаки и построение дерева атаки [2]. На данном этапе операция проводится экспертом,

который определяет элементы дерева исходя из задач системы безопасности организации и требований стандартов/законодательства. Дерево удобно представить в текстовом виде:

db info confidentiality loss
1. site 1 (OR)
1.1. DB
1.1.1. remote attack (AND)
1.1.1.1. network access (OR)
1.1.1.1.1. break through boundary
1.1.1.1.2. Access through Chanel 1
1.1.1.1.3. Access through Chanel 2
1.1.1.2. OR
1.1.1.2.1. login to db (OR)
1.1.1.2.1.1. steal credentials from user (OR)
1.1.1.2.1.1.1. steal from PC
1.1.1.2.1.1.1.1. virus/trojan
1.1.1.2.1.1.1.2. physically steal (AND)
1.1.1.2.1.1.1.2.1. password written down
1.1.1.2.1.1.1.2.2. physical access to OFFICE
1.1.1.2.1.2. intercept credentials from network
1.1.1.2.2. break into db
1.1.1.2.2.1. vulnerability
1.1.2. physically steal info
1.1.2.1. access to site 1
1.2. Tape Library
1.2.1. remote attack (AND)
1.2.1.1. network access (OR)
1.2.1.1.1. break through boundary
1.2.1.1.2. Access through Chanel 1
1.2.1.1.3. Access through Chanel 2
1.2.1.2. OR
1.2.1.2.1. login to library (OR)
1.2.1.2.1.1. steal credentials from user (OR)
1.2.1.2.1.1.1. steal from PC
1.2.1.2.1.1.1.1. virus/trojan
1.2.1.2.1.1.1.2. physically steal (AND)
1.2.1.2.1.1.1.2.1. password written down
1.2.1.2.1.1.1.2.2. physical access to OFFICE
1.2.1.2.1.2. intercept credentials from network
1.2.1.2.2. break into library
1.2.1.2.2.1. vulnerability
1.2.2. physically steal info
1.2.2.1. access to site 1
2. site 2
2.1. DB
2.1.1. remote attack (AND)
2.1.1.1. network access (OR)

2.1.1.1.1. break through boundary
2.1.1.1.2. Access through Chanel 2
2.1.1.1.3. Access through Chanel 3
2.1.1.2. OR
2.1.1.2.1. login to db (OR)
2.1.1.2.1.1. steal credentials from user (OR)
2.1.1.2.1.1.1. steal from PC
2.1.1.2.1.1.1.1. virus/trojan
2.1.1.2.1.1.1.2. physically steal (AND)
2.1.1.2.1.1.1.2.1. password written down
2.1.1.2.1.1.1.2.2. physical access to OFFICE
2.1.1.2.1.2. intercept credentials from network
2.1.1.2.2. break into db
2.1.1.2.2.1. vulnerability
2.1.2. physically steal info
2.1.2.1. access to site 2
3. office
3.1. steal from user's PC
4. chanel 1
4.1. intercept data
5. chanel 2
5.1. intercept data
6. chanel 3
6.1. intercept data

Как мы видим, даже в случае небольшого (и ограниченного) примера дерево носит достаточно объемный характер, однако построение его облегчается тем, что многие блоки являются типовыми и их можно использовать множество раз, возможно с небольшими поправками (см., например: Site 1 — DB и Site 2 — DB).

Следующим шагом является определение метрик, по которым, собственно, и будет проводиться оценка. Рассмотрим небольшой фрагмент дерева, изображенный на рис. 2.

1.2.1.2.1.1. steal credentials from user (OR)
1.2.1.2.1.1.1. steal from PC
1.2.1.2.1.1.1.1. virus/trojan

Элементом нижнего уровня (т. е. концевым узлом, или листом) данного фрагмента дерева является элемент «virus/trojan», обозначающий путь атаки на клиентский компьютер.

Для оценки этого элемента необходимо связать с ним знания о методах защиты от данной угрозы. Значения в прямоугольниках под компонентами выражают относительные веса критериев. Veto обозначает, что критерий является необходимым. Pass означает, что группа критериев является достаточной.

Следующим шагом является непосредственная оценка значений критериев и агрегация. Рассмотрим вышеприведенный пример. Предположим, в организации существует следующая ситуация (значения в скобках соответствуют численным выражениям высказываний по шкале [0,1]):

1. Используются ОС Windows ($A_{OS} = 0$);

2. Антивирусы установлены на всех рабочих станциях и регулярно обновляются ($A_{AV} = 0.98$);

3. Происходит регулярная установка обновлений ОС, впрочем, пользователь может отсрочить связанную с этим перезагрузку на несколько дней (в пределах недели) ($A_{Up} = 0.9$);

4. Пользователям запрещено самостоятельно устанавливать ПО ($A_{SW} = 0.98$);
5. Производится фильтрация спама ($A_{SP} = 0.8$).

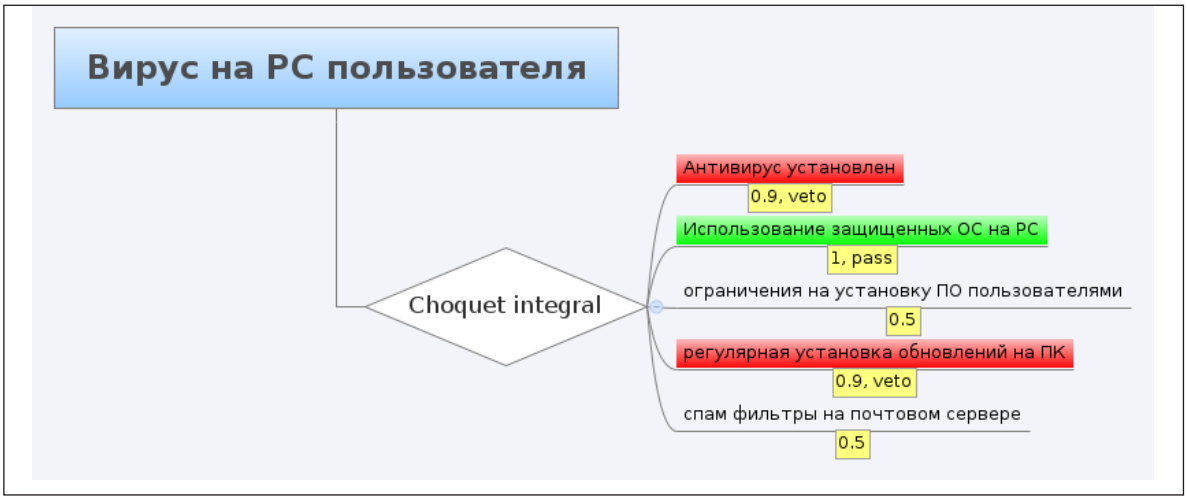

Рис. 2. Элемент дерева атаки, необходимые и достаточные компоненты

Составим таблицу весов (предварительно нормализовав их). Мы считаем, что использование защищенных ОС в данном примере является достаточным критерием даже в отсутствие антивирусной защиты и проведения обновлений ПО и, наоборот, таким образом, нечеткая мера всех множеств, включающих OS, равняется одному, так же как и множества {AV,UP,SP,SW}. Оператор обладает достаточной гибкостью для любого сочетания необходимых и достаточных условий, в соответствии с семантическими требованиями (см. ниже).

	μ		μ
{}	0	{OS,AV,UP}	1
{OS}	1	{OS,AV,SW}	1
{AV}	0	{OS,AV,SP}	1
{UP}	0	{OS,UP,SW}	1
{SW}	0	{OS,UP,SP}	1
{SP}	0	{OS,SW,SP}	1
{OS,AV}	1	{AV,UP,SW}	0.82
{OS,UP}	1	{AV,UP,SP}	0.82
{OS,SW}	1	{AV,SW,SP}	0
{OS,SP}	1	{UP,SW,SP}	0
{AV,UP}	0.64	{OS,AV,UP,SW}	1
{AV,SW}	0	{OS,AV,UP,SP}	1
{AV,SP}	0	{OS,AV,SW,SP}	1
{UP,SW}	0	{OS,UP,SW,SP}	1
{UP,SP}	0	{AV,UP,SW,SP}	1
{SW,SP}	0	{OS,AV,UP,SW,SP}	1

Индекс Шепли для агрегируемых переменных выглядит следующим образом. Пропорции весов несколько изменились, что произошло ввиду объявления компонентов A_{av} и A_{up} необходимыми.

$$u_{OS}(м) = 0.6966667$$

$$u_{AV}(м) = 0.1366667$$

$$u_{UP}(м) = 0.1366667$$

$$u_{SW}(м) = 0.015$$

$$u_{SP}(м) = 0.015$$

Интеграл Шоке

$$C_м(A_{OS}, A_{AV}, A_{UP}, A_{SP}, A_{SW}) = 0.882$$

Значение находится в пределах [min(X),max(X)], как и предполагалось.

Зависимость значения интеграла от значений отдельных критериев

Проанализируем влияние компонента OS на общее значение и продемонстрируем, как изменяется поведение оператора при изменении нечеткой меры. Для этого зафиксируем все критерии кроме данного и построим график значения интеграла Шоке (Рис. 3).

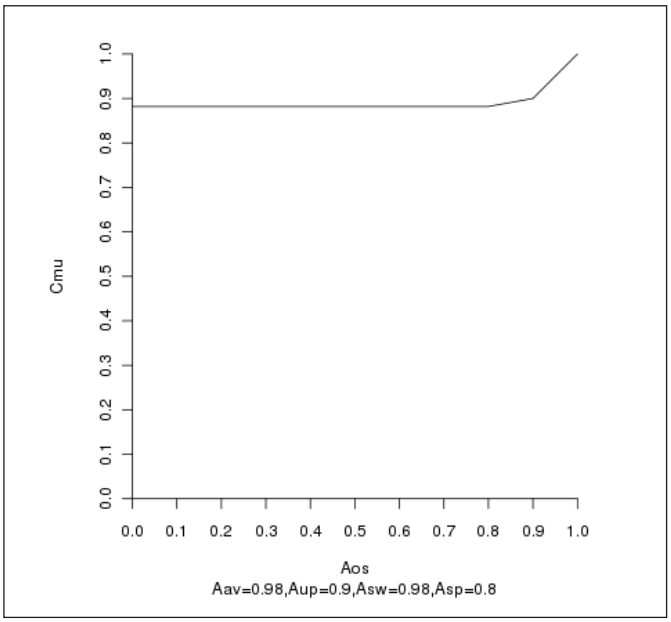

Рис. 3. Зависимость агрегированного значения от величины компонента OS

Теперь предположим, что использование защищенной ОС более не является достаточным условием при отсутствии проведения обновлений ПО. В терминах нечеткой меры это означает, что теперь мы присваиваем единицу только тем множествам, которые включают не только OS, но и UP, новые значения нечеткой меры приведены в таблице 2.

	μ		μ
{}	0	{OS,AV,UP}	1
{OS}	0	{OS,AV,SW}	0
{AV}	0	{OS,AV,SP}	0
{UP}	0	{OS,UP,SW}	1
{SW}	0	{OS,UP,SP}	1
{SP}	0	{OS,SW,SP}	0
{OS,AV}	0	{AV,UP,SW}	0.82
{OS,UP}	1	{AV,UP,SP}	0.82
{OS,SW}	0	{AV,SW,SP}	0
{OS,SP}	0	{UP,SW,SP}	0
{AV,UP}	0.64	{OS,AV,UP,SW}	1

{AV,SW}	0	{OS,AV,UP,SP}	1
{AV,SP}	0	{OS,AV,SW,SP}	0
{UP,SW}	0	{OS,UP,SW,SP}	1
{UP,SP}	0	{AV,UP,SW,SP}	1
{SW,SP}	0	{OS,AV,UP,SW,SP}	1

График наглядно иллюстрирует (Рис. 4), что до определенного значения функции ведут себя одинаково, однако в дальнейшем агрегированное значение, имеющее требование наличия критерия UP, ограничивается сверху его значением (0.9), что соответствует установленным ограничениям.

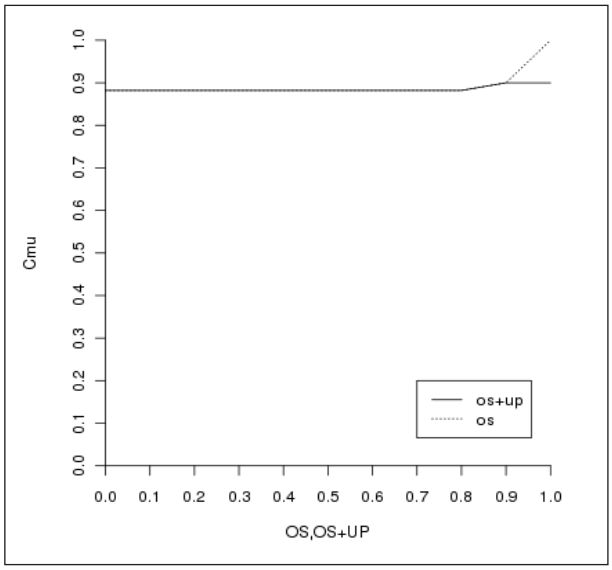

Рис. 4. Расширение свойства необходимости на сочетание двух критериев

Выводы

В статье продемонстрирован подход к моделированию риска с использованием теории нечеткой меры, рассмотрен практический пример и проиллюстрированы математические свойства интеграла Шоке в применении к решаемой задаче. В дальнейшем будет проведено сравнение данного подхода с классическим решением, использующим байесовы сети.

СПИСОК ЛИТЕРАТУРЫ:

1. *Тимонин М. В., Лаврентьев В. С.* Использование теории нечеткой меры для агрегации составляющих риска информационной безопасности (в печати).
2. *Schneier B.* Attack Trees. 1999. URL: http://www.schneier.com/paper-attacktrees-ddj-ft.html.