ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ НЕЧЁТКОЙ ЛОГИКИ

Чопик К.В. Фролов А.К.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Алефиренко В.М. – канд.техн.наук

Предложен метод оценки защищенности информационной системы, позволяющий оперативно регулировать порог формирования сигнала тревоги и предоставляющий количественную и качественную оценку защищенности сети. Проведена оценка защищенности на конкретном примере.

В настоящее время информация имеет огромную ценность, которая определяется прибылью, получаемой при ее использовании, или ущербом, который может быть нанесен информационной системе предприятия в случае использования ее злоумышленниками.

В связи с этим остро встает вопрос оценки защищенности всей информационной системы в целом. Произведя такую оценку, можно выбрать наиболее эффективную систему защиты как с функциональной, так и с экономической точки зрения в каждом конкретном случае [1].

При оценке защищенности информационной системы на основе нечеткой логики рассматриваются четыре составляющие, на основании оценки которых осуществляется формирование сигнала тревоги или снижается уровень защищенности.

Такими составляющими являются [2]:

– уровень атаки;

– критичность актива устройства сети;

– уровень доверия сообщающему устройству;

– уровень защиты устройств сети.

Под уровнем атаки подразумевается оценка степени вредоносности атаки, представленная в терминах нечеткой логики «низкий – средний – высокий».

Критичность активов устройств сети определяется в результате оценки ресурсов, обрабатываемых на каждом устройстве.

Уровень доверия сообщающему устройству определяется с целью повышения достоверности выявления атак.

Уровень защиты устройств сети позволяет сократить количество сигналов тревоги. То есть, если известно, что устройство сети имеет высокий уровень защиты, то не следует уделять инциденту информационной безопасности пристального внимания в режиме реального времени.

Данные параметры позволяют оценить важность инцидента информационной безопасности (ИБ) устройства сети, которая определяется по формуле [2]:

$$I_{ЛВС}=k(m)\cdot At\cdot As\cdot P_{УС}\cdot T, \quad (1)$$

где k(m) – нормирующий коэффициент, позволяющий представить полученный результат в диапазоне [0; 1]. Для параметров информационной безопасности с 5-ти уровневой градацией k(m) =0,0016; At – уровень атаки; As – критичность активов устройств сети; $P_{УС}$ – уровень защиты; T – уровень доверия сообщающему устройству.

Для применения формулы (1) необходимо произвести преобразования нечетких переменных, после которых каждой нечеткой переменной будет соответствовать положительное целое число в диапазоне [1; 5]. Приведем в соответствие для каждого параметра его качественную характеристику с количественной. Для параметров «уровень атаки» и «критичность активов устройств сети» качественной оценке «Очень низкий» соответствует количественное значение «1», «Низкий» – «2», «Средний» – «3», «Высокий» – «4», «Очень высокий» – «5». Для параметров «Уровень доверия сообщающему устройству» и «Уровень защиты устройств сети» качественной оценке «Очень низкий» соответствует количественное значение «5», «Очень высокий» – «1».

Зная важность инцидентов ИБ для каждого устройства сети, можно получить числовую оценку уровня защищенности ИС в целом по формуле [2]:

$$P_{ИС}=\prod_{i=1}^{n} 1-I_{УСi}\ , \quad (2)$$

где n – количество устройств сети в ИС; $I_{УСi}$ – важность инцидента ИБ i-го устройства сети.

На основе значений количественной оценки защищенности ИС можно получить значения качественной оценки защищенности ИС. Если значение $P_{ИС}$ находится в диапазоне [0;0,5) это говорит об очень низкой защищенности ИС, если $P_{ИС}$ находится в диапазоне [0,5;0,7) – низкой, [0,7;0,85) – средней, [0,85;0,95) – высокой, [0,95;1] – очень высокой защищенности ИС.

Рассмотрим простую компьютерную сеть, представленную на рисунке 1, и проведём оценку её защищенности. Данная сеть состоит из четырех компьютеров, одного сервера и одного коммутатора.

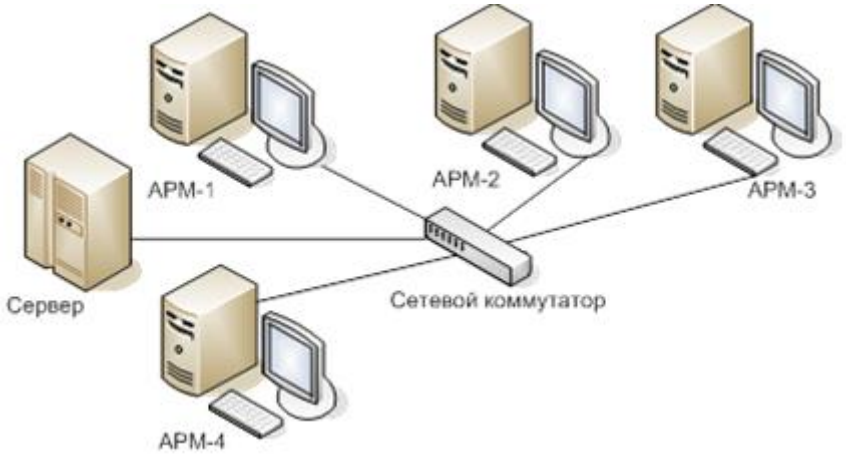

Рисунок 1 – Топология оцениваемой компьютерной сети

Пусть компьютеры имеют следующие показатели:
– уровень атаки «высокий – 4»;
– критичность активов устройств сети «средняя – 3»;
– уровень защиты «средний – 3»;
– уровень доверия сообщающему устройству «очень высокий – 1».
Для сервера:
– уровень атаки «очень высокий – 5»;
– критичность активов устройств сети «высокая – 4»;
– уровень защиты «высокий – 2»;
– уровень доверия сообщающему устройству «очень высокий – 1».
Для коммутатора:
– уровень атаки уровень атаки «очень высокий – 5»;
– критичность активов устройств сети «очень высокая – 5»;
– уровень защиты «высокий – 2»;
– уровень доверия сообщающему устройству «очень высокий – 1»;
Порог $Р_{ИС}$* заданный системным администратором сети примем 0,8.
Теперь получим числовую оценку уровня защищенности ИС по формуле 2:

$$Р_{ИС}=(1-0{,}0016\cdot 4\cdot 3\cdot 3\cdot 1)^4\cdot(1-0{,}0016\cdot 5\cdot 4\cdot 2\cdot 1)\cdot(1-0{,}0016\cdot 5\cdot 5\cdot 2\cdot 1)=0{,}679$$

Данный результат показывает, что уровень защищенности данной сети низкий, так как $Р_{ИС}$ находится в диапазоне [0,5;0,7). Поскольку значение $Р_{ИС}$ не превышает заданный порог $Р_{ИС}$*, то система оценки уведомит системного администратора об инцидентах информационной безопасности и отобразит при этом как качественную оценку защищенности ИС («низкий»), так и количественную («0,679»).

Преимуществом данного метода является простота реализации. Метод применим для компьютерных сетей любой топологии.

Недостатком данного метода является тот факт, что параметры важности инцидента для каждого устройства сети определяются системным администратором, то есть присутствует человеческий фактор, из-за которого может понизиться точность оценки защищенности ИС в случае недостаточной квалификации системного администратора.

Таким образом, предложенный метод оценки защищенности ИС позволяет быстро регулировать порог формирования сигнала тревоги. При этом, результатом системы оценки защищенности ИС является как количественная, так и качественная оценки защищенности.

Список использованных источников:

1. Оценка защищенности [Электронный ресурс]. – Режим доступа: http://op.vlsu.ru/fileadmin/Programmy/Magistratura/10.04.01/Metod_doc/Uch_posob/2016/Metod_OcenkaZash_100401_29122016.pdf.

2. Файзуллин, Р.Р. Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечеткой логики / Р. Р. Файзуллин, В.И. Васильев // сб. публикаций научного журнала «Вестник УГАТУ». – 2013.. – Т.17, N2 (55). – С. 150 – 156.