УДК 007.52/007.5

МЕТОДИКА ЛОКАЛИЗАЦИИ УЧАСТКА КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ С АНОМАЛЬНЫМ ПОВЕДЕНИЕМ*

METHODIC OF LOCALIZATION OF A SITE OF A CORPORATE NETWORK WITH ANOMALOUS BEHAVIOR

М.М. МОНАХОВА, А.А. ПОРФИРЬЕВ, Г.В. ПУТИНЦЕВ, И.С. МАРКОВ, Д.А. ШЕРУНТАЕВ
M.M. MONAKHOVA, A.A. PORFIRYEV, G.V. PUTINTSEV, I.S. MARKOV, D.A. SHERUNTAYEV

(Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых)
(Vladimir State University named after Alexander and Nikolai Stoletovs)
E-mail: mariya.monakhova@gmail.com; denissheruntaev@mail.ru; markoffken@yahoo.com; putigr@mail.ru; lordtid@yandex.ru

В статье предлагается метод обнаружения участка корпоративной сети передачи данных с возникшим инцидентом информационной безопасности. Вводятся понятия характеристик математической модели сети, приводятся примеры эталонных и текущих расчетных матриц метрик, объясняется актуальность данного представления и работы в целом.

In this article reviewing of a method of detection of a section of a corporate data communication network with the arisen incident of information security is offered. Concepts of characteristics of a mathematical model of a network are entered, examples of reference and current estimated matrixes of metrics are given, and the relevance of this representation and operation in general speaks.

Ключевые слова: информационная безопасность, корпоративная сеть передачи данных, инцидент информационной безопасности, маршрутизация, аномальное поведение сети.

Keywords: information security, corporate data transmission network, information security incident, routing, abnormal network behavior.

Корпоративная сеть передачи данных (КСПД) представляет собой основную интегративную техническую платформу информационного взаимодействия в рамках производственных, экономических, хозяйственных и других процессов современных предприятий текстильной промышленности [1]. Как правило, именно на КСПД приходится наибольшее количество деструктивных воздействий – естественных угроз информационной безопасности (ИБ), что влечет за собой нарушения ее (КСПД) функционирования и, как следствие, увеличение рисков ИБ предприятия [2...4]. На рис. 1 мы видим типовой упрощенный граф подсетей сетевого уровня подели OSI КСПД. На графе КСПД сетевого уровня модели OSI находим подсети (W), непосредственно подсоединенные между собой, то есть имеющие общий узел. На пересечении данных подсетей в начальную матрицу графа M ставим значение, равное "1", символизирующее стандартное значение метрики "directly connected", то есть непосред-

* Статья подготовлена в рамках выполнения научно-исследовательских работ, поддержанных грантами Российского фонда фундаментальных исследований № 16-47-330055, № 18-07-01109.

ственно присоединенные, в сетевой маршрутизации. Для связи внутри одной подсети, то есть W1-W1, примем значение, также равное 1. Данные преобразования представлены в табл. 1 (преобразованная матрица графа подсетей КСПД).

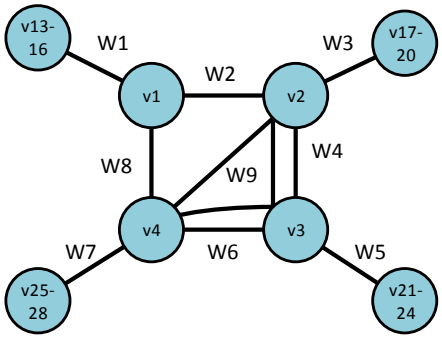

Рис. 1

Таблица 1

	W1	W2	W3	W4	W5	W6	W7	W8	W9
W1	1	1	0	0	0	0	0	1	0
W2	1	1	1	1	0	0	0	1	1
W3	0	1	1	1	0	0	0	0	1
W4	0	1	1	1	1	1	0	0	1
W5	0	0	0	1	1	1	0	0	1
W6	0	0	0	1	1	1	1	1	1
W7	0	0	0	0	0	1	1	1	1
W8	1	1	0	0	0	1	1	1	1
W9	0	1	1	1	1	1	1	1	1

Оставшиеся нулевые связи мы должны заполнить значением метрик действующего в сети протокола маршрутизации по следующими правилам:

- производим попытку соединения с маршрутизатором для получения значения параметров действующего в сети протокола маршрутизации и дальнейшего расчета метрики на основе этих параметров. Если маршрутизатор не отвечает, то значение метрики на соединении опрашиваемых подсетей примем равным "NULL";

- производим попытку соединения с маршрутизатором для получения значения параметров действующего в сети протокола маршрутизации и дальнейшего расчета метрики на основе этих параметров. Если маршрутизатор доступен, получаем значения параметров протокола маршрутизации и производим расчет метрики данного протокола. Заносим в матрицу М на пересечение опрашиваемых подсетей подсчитанное значение метрики действующего в сети протокола маршрутизации. Для подсчета метрики действующего в сети протокола маршрутизации воспользуемся формулами для расчета метрик протокола EIGRP. Для получения данных значений параметров действующего в КСПД протокола маршрутизации требуется произвести удаленное подключение к маршрутизирующему оборудованию.

Для построения эталонной матрицы метрик требуется произвести n замеров метрик, где n является отношением общей величины временного интервала к величине промежутка времени между замерами: $n = \frac{|T|}{w}$, где $|T|$ – общая величина временного интервала; w – величина промежутка времени, через который производится замер. В результате получаем множество значений метрик действующего в КСПД протокола маршрутизации: $p_{ij} = \{p_{ij}[1], \dots, p_{ij}[n]\}$, где i – номер подсети, из которой ведется опрос; j – номер подсети, в которую запрашивается метрика; p_{ij} – значение метрики на соединении подсетей; n – количество замеров метрик на протяжении временного интервала.

Конечным эталонным значением метрики действующего в КСПД протокола маршрутизации является интервал – математическое ожидание величины метрик плюс/минус среднеквадратичное отклонение: $M_{ij}^{ЭТ} = M\left[p_{ij}\right] \pm \delta$, где $M\left[p_{ij}\right]$ – математическое ожидание величин метрик из i в j подсеть; δ – среднеквадратичное отклонение данной величины. Конечная эталонная матрица значений метрик функционирующего в КСПД динамического протокола маршрутизации представлена в табл. 2.

Эталонная матрица метрик строится для каждого временного интервала сетевой активности пользователей КСПД при условии настроенной КСПД, отсутствии ошибок функционирования, а также без вмешательства внешних помех, искажающих параметры сетевой активности временного интервала.

Таблица 2

	W1	W2	W3	W4	W5	W6	W7	W8	W9
W1	1	1	$M[p_{1,3}] \pm \delta$	$M[p_{1,4}] \pm \delta$	$M[p_{1,5}] \pm \delta$	$M[p_{1,6}] \pm \delta$	$M[p_{1,7}] \pm \delta$	1	$M[p_{1,9}] \pm \delta$
W2	1	1	1	1	$M[p_{2,5}] \pm \delta$	$M[p_{2,6}] \pm \delta$	$M[p_{2,7}] \pm \delta$	1	1
W3	$M[p_{3,1}] \pm \delta$	1	1	1	$M[p_{3,5}] \pm \delta$	$M[p_{3,6}] \pm \delta$	$M[p_{3,7}] \pm \delta$	$M[p_{3,8}] \pm \delta$	1
W4	$M[p_{4,1}] \pm \delta$	1	1	1	1	1	$M[p_{4,7}] \pm \delta$	$M[p_{4,8}] \pm \delta$	1
W5	$M[p_{5,1}] \pm \delta$	$M[p_{5,2}] \pm \delta$	$M[p_{5,3}] \pm \delta$	1	1	1	$M[p_{5,7}] \pm \delta$	$M[p_{5,8}] \pm \delta$	1
W6	$M[p_{6,1}] \pm \delta$	$M[p_{6,2}] \pm \delta$	$M[p_{6,3}] \pm \delta$	1	1	1	1	1	1
W7	$M[p_{7,1}] \pm \delta$	$M[p_{7,2}] \pm \delta$	$M[p_{7,3}] \pm \delta$	$M[p_{7,4}] \pm \delta$	$M[p_{7,5}] \pm \delta$	1	1	1	1
W8	1	1	$M[p_{8,3}] \pm \delta$	$M[p_{8,4}] \pm \delta$	$M[p_{8,5}] \pm \delta$	1	1	1	1
W9	$M[p_{9,1}] \pm \delta$	1	1	1	1	1	1	1	1

По аналогичному принципу строятся текущие значения метрик по каждому временному интервалу, непосредственно в момент проверки состояния КСПД. Затем происходит сравнение матрицы текущих значений метрик с эталонной матрицей значения метрик. Для сравнения выбирается эталонная матрица значений метрик того же временного интервала сетевой активности, в период которой был произведен съем текущей матрицы.

Построим квадратную матрицу сравнения $C = m \cdot m$, где $m = |W|$. Правила присвоения значений ячейкам матрице сравнения C:

– Сравнение значений метрик "directly connected": если значение "directly connected" текущей матрицы не совпадает со значением эталонной матрицы, то в матрицу сравнения записываем значение, равное "0"; иначе записываем "1";

– Сравнение значений метрик: если текущая метрика лежит ниже эталонного интервала значений, то в матрицу сравнения записываем значение данной метрики; иначе записываем разницу текущей метрики с верхней границей интервала; если текущая метрика лежит в эталонном интервале, то в матрицу сравнения записываем значение, равное 1.

$$\begin{cases} M_{ij}^{тек} < M\left[p_{ij}\right] - \delta; \ C_{ij} = 2, \\ M_{ij}^{тек} > M\left[p_{ij}\right] + \delta; \ C_{ij} = 0, \\ M_{ij}^{тек} \in M\left[p_{ij}\right] \pm \delta; \ C_{ij} = 1. \end{cases}$$

Далее выполняется определение сегмента КСПД с нарушением политики ИБ. На основе матрицы сравнения C определяем подсети доступ, к которым был потерян следующим способом.

Алгоритм определения критичности сегмента КСПД:

Последовательно выбираем подсеть. Производим подсчет количества связей $C_{ij} = 0$, лежащих выше эталонного интервала значений n_0. Производим подсчет количества связей $C_{ij} = 2$, лежащих ниже эталонного интервала n_2. Производим подсчет количества связей $C_{ij} = 1$, лежащих в эталонном интервале значений n_1. Выделяем приоритеты значимости для каждого типа значений матрицы сравнения C_{ij}. Произведем сопоставление значений RGB (Red, Green, Blue – адаптивная цветовая модель) с типами значений матрицы сравнения следующим образом:

$$\begin{cases} R = \frac{255n_0}{n} p_0, \\ G = \frac{255n_1}{n} p_1, \\ B = \frac{255n_2}{n} p_2, \end{cases}$$

где n – количество подсетей; $p_0 = 2$; $p_1 = 0{,}5$; $p_2 = 1$.

Производим построение упрощенного графа КСПД, окрашивая сегменты сети в соответствии с полученными значениями RGB. Для информативности графа обозначим вес ребра в формате $n_0/n_1/n_2$. В результате выполнения алгоритма получаем матрицу сравнения. На основе полученной матрицы сравнения произведем построение графа КСПД с указанием критичных сегментов, построенный граф представлен на рис. 2.

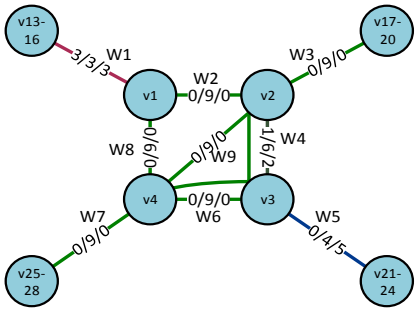

Рис. 2

Как мы можем видеть из графа – красным цветом указаны критичные области, подверженные влиянию инцидента, синим – области с возможным нарушением ИБ, а зеленым – участки с нормальным функционированием КСПД. Данный граф может быть передан Администратору безопасности для проведения дополнительных проверок или для выявления инцидента ИБ и устранения аномального поведения сети.

ЛИТЕРАТУРА

1. *Басов Д.В., Черноверская В.В.* Интегрированная среда разработки системы управления распределенными объектами // Вестник Московского гос. ун-та приборостроения и информатики. – 2012.

2. *Nikitin O., Monakhova M.* About forming of profile of TCN / O. Nikitin and other – Problems of efficiency and safety of functioning of the difficult technical and informative systems // Materials of XXIII Russian scientific and technical conference. Serpukhov: Branch MA of SRF. – 2014. P. 190...193.

3. *Путинцев Г.В., Монахова М.М.* Автоматизированная система обнаружения инцидентов информационной безопасности корпоративных сетей передачи данных // Сб. докл. VII Всерос. научн.-практ. конф.: Имитационное моделирование. – 2015, С.145...146.

4. *Монахова М.М., Порфирьев А.А., Мазурок Д.В., Путинцев Г.В.* Система обеспечения визуальной коммуникации по защищенным каналам связи // Проблемы современной науки и образования. – 2017, № 5 (87).

REFERENCES

1. Basov D.V., Chernoverskaja V.V. Integrirovannaja sreda razrabotki sistemy upravlenija raspredelennymi ob"ektami // Vestnik Moskovskogo gos. un-ta priborostroenija i informatiki. – 2012.

2. Nikitin O., Monakhova M. About forming of profile of TCN / O. Nikitin and other – Problems of efficiency and safety of functioning of the difficult technical and informative systems // Materials of XXIII Russian scientific and technical conference. Serpukhov: Branch MA of SRF. – 2014. P. 190...193.

3. Putincev G.V., Monahova M.M. Avtomatizirovannaja sistema obnaruzhenija incidentov informacionnoj bezopasnosti korporativnyh setej peredachi dannyh // Sb. dokl. VII Vseros. nauchn.-prakt. konf.: Imitacionnoe modelirovanie. – 2015, S.145...146.

4. Monahova M.M., Porfir'ev A.A., Mazurok D.V., Putincev G.V. Sistema obespechenija vizual'noj kommunikacii po zashhishhennym kanalam svjazi // Problemy sovremennoj nauki i obrazovanija. – 2017, № 5 (87).

Рекомендована кафедрой информатики и защиты информации. Поступила 06.06.18.