АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Г.В. Путинцев, М.М. Монахова (Владимир)

Проблема обеспечения безопасности корпоративных сетей передачи данных (КСПД) в настоящее время широко обсуждается как в отечественной науке и промышленности, так и за рубежом. Это обусловлено рядом причин, таких как:

- структурная сложность и размерность современных КСПД;
- возрастающие требования к уровню информационной безопасности (ИБ) как компонентов, так и всей КСПД, особенно предназначенных для работ на опасных промышленных объектах.

Одной из основных составляющих процесса обеспечения безопасности КСПД является локализация и устранение аномалий ее функционирования, наиболее значимыми аномалиями здесь выделим отклонения от штатного функционирования компонентов КСПД и перегрузки в каналах связи.

Автоматизированная система обнаружения инцидентов (АСОИн) ИБ представляет собой комплекс модулей, программ и алгоритмов, направленных на выявление участков аномального функционирования КСПД.

АСОИн ИБ позволяет за незначительное время выявить зону аномального поведения КСПД, тем самым позволит администратору безопасности локализовать ее и не допустить дальнейшего распространения пораженных инцидентом (инцидентами) ИБ участков, а также снизить время на поиск и устранение инцидента ИБ путем выявления критичных узлов сети.

Структурно АСОИн ИБ состоит из четырех подсистем.

Концептуальная схема АСОИн ИБ приведена на рис. 1

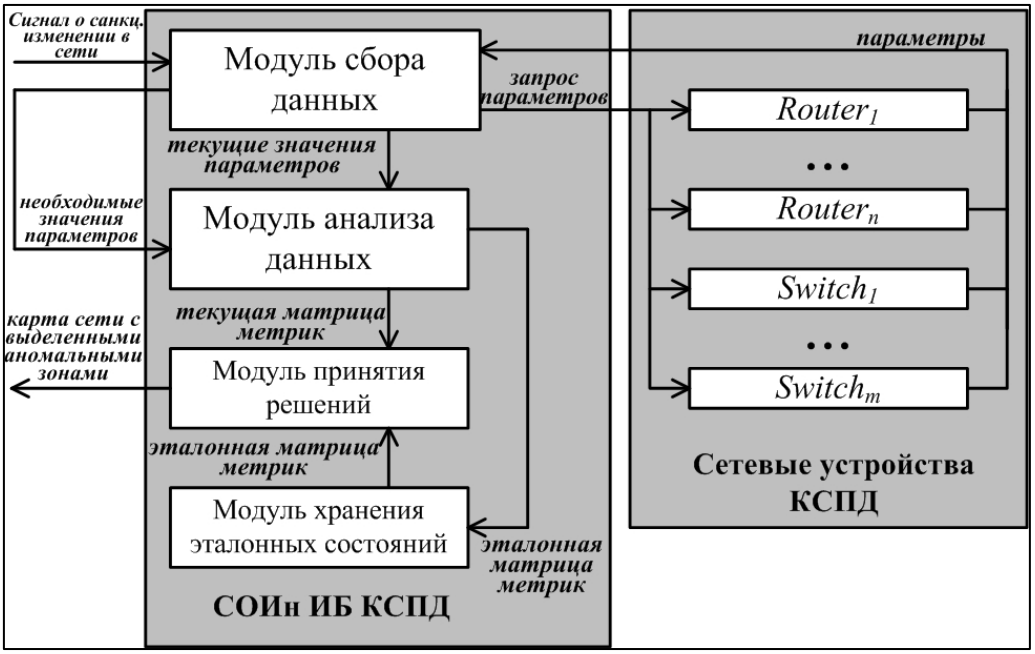

Рис. 1- Структурная схема АСОИн ИБ КСПД

Модули АСОИн ИБ имеют следующую функциональность:

- Модуль сбора данных (МСД), во-первых, собирает значения параметров элементов КСПД для создания эталонной матрицы метрик. Во-вторых, МСД собирает новые значения параметров элементов КСПД в случае санкционированных изменений в сети (после предварительной настройки сети сетевыми администраторами). В-третьих, МСД собирает текущие значения параметров элементов КСПД для их последующей обработки. Сбор значений параметров выполняется путем отправления запроса на элементы сети и получения ответов в виде dump-файлов, содержащих необходимые характеристики.
- Модуль анализа данных (МАД) обрабатывает поступившие на него dump-файлы, извлекая из них значения параметров, и путем математических вычислений производит расчет текущей и эталонной матриц метрик.
- Модуль принятия решений сопоставляет текущую и эталонную матрицы метрик и, используя алгоритмы, принимает решения по выявлению критических мест в сети. Затем выдает администратору ИБ карту - граф сети с выделенными на ней зонами аномального функционирования сети.
- Модуль хранения эталонных состояний представляет собой базу данных, содержащую эталонные значения параметров КСПД и эталонную матрицу метрик.

Концептуально важным в функционировании АСОИн ИБ является составление эталонной и текущей матриц метрик. Матрица метрик ***M***, $|M|=m*m$, где $|M|$ - количество различных ВС внутри КСПД. Строится матрица М по следующему алгоритму.

Например, имеется КСПД (рис.2). Граф сетевого уровня изображен на рисунке 3. Заметим, что на графе отсутствуют устройства, не функционирующие на сетевом уровне, такие, как коммутаторы второго уровня (SW1 – SW4). Множество U на графе представляет собой совокупность таких множеств, как R, PK и S (маршрутизаторов, рабочих станций и серверов). Для наглядности все вычислительные сети на графе выделены цветом.

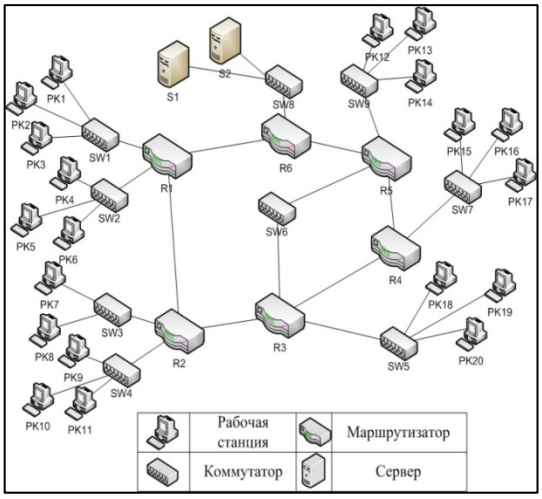

Рис. 2 - схема **тестовой** КСПД

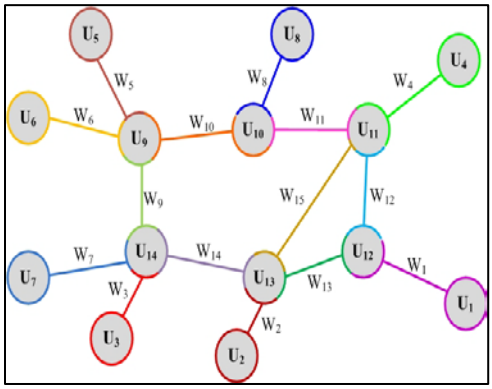

Рис. 3 - граф сетевого уровня рассматриваемой КСПД с выделеными ВС

Здесь строится граф F=(W, H) (рис. 4), где узлами графа W будут являться ВС, а ребрами H – логические соединения между сетями (вне зависимости от маршрута). Отметим, что граф будет характеризоваться следующими особенностями:

- в большинстве случаев данный граф будет полносвязным, т.к. внутри одной КСПД имеется связь всех ВС между собой (если иное не предусмотрено политикой безопасности, такими факторами, как установленный ACL, межсетевой экран и т.д.). В связи с этим было принято построить полносвязный граф, а в случае отсутствия связи между ВС вес ребра принять равным нулю;
- в случае использования различных протоколов маршрутизации, либо разделения внутри протоколов КСПД на различные автономные системы, строятся разные матрицы, соответственно и разные графы для каждого протокола/системы;
- на данном шаге примем все веса ребер равными нулю.

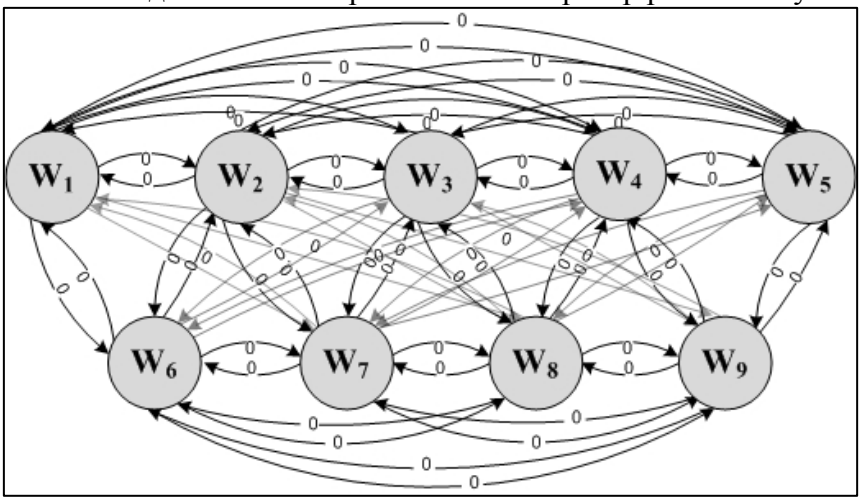

Рис. 4 - пример графа межсетевого взаимодействия сегмента рассматриваемой КСПД

«Взвесим» ребра ранее построенного графа F, для удобства перейдя от графового представления к матричному. Построим квадратную матрицу M=m*m, где m=|W| (таблица 1). По умолчанию все значения в матрице примем равные нулю.

	W_1	…	W_m
W_1	0	0	0
…	0	0	0
W_m	0	0	0

Таблица 1 Начальный этап построения матрицы M

Заполним нулевые ячейки. Для расчета метрик воспользуемся формулой расчета метрики того протокола, который функционирует в данной сети.

Для того, чтобы вычислить значения метрик при помощи измерителя снимем данные (dump-файлы) с маршрутизирующих устройств и подставим их в формулу. Рассчитаем значения и получим матрицу вида (таблица 3):

	W_1	…	…	…	…	W_m
W_1	1	X^2_1	1	X^4_1	X^5_1	X^6_1
…	X^1_2	1	X^3_2	1	X^5_2	X^6_2
…	1	X^2_3	1	1	X^5_3	X^6_3
…	X^1_4	1	1	1	X^5_4	X^6_4
…	X^1_5	X^2_5	X^3_5	X^4_5	1	1
W_m	X^1_6	X^2_6	X^3_6	X^4_6	1	1

Таблица 3 Текущая матрица метрик M

Здесь, единицей отмечены те сети, которые являются непосредственно подключенными, как стандартное значение метрики «directly connected» (непосредственно присоединенные) в сетевой маршрутизации. Для связей внутри одной сети ($\mathbf{W_1}$-$\mathbf{W_1}$) метрику так же примем равной единице

В случае, если строится эталонная матрица (измерители снимали данные с настроенной КСПД при отсутствии ошибок в сети и при эмуляции типичной сетевой активности без вмешательства внешних помех), необходимо записать ее в модуль хранения эталонных состояний и вернуться к шагу 1. В противном случае (в случае, если полученная матрица является отображением текущего состояния КСПД) необходимо продолжить выполнение алгоритма.

Выполним сравнение полученной матрицы с эталонной.

Предположим, эталонная матрица ($M_{эт}$)имеет вид (таблица 4):

	W_1	…	…	…	…	W_m
W_1	1	Y^2_1	1	Y^4_1	Y^5_1	Y^6_1
…	Y^1_2	1	Y^3_2	1	Y^5_2	Y^6_2
W_m	Y^1_6	Y^2_6	Y^3_6	Y^4_6	1	1

Таблица 4 Эталонная матрица метрик $M_{эт}$

Получим итоговую матрицу сравнения (таблица 5) L, где L[I,j] = {0,1} следующим образом:

$$\forall \mathbf{M[i,j]}\ \exists \mathbf{L[i,j]}, \begin{cases} \mathbf{L[i,j]=0} \leftrightarrow \mathbf{M[i,j]} \neq \text{Мэт}\ \mathbf{[i,j]} \\ \mathbf{L[i,j]=1} \leftrightarrow \mathbf{M[i,j]} = \text{М}_{эт}\mathbf{[i,j]} \end{cases} \quad \textbf{(1)}$$

	W_1	…	…	…	…	W_m
W_1	1	L^2_1	1	L^4_1	L^5_1	L^6_1
…	L^1_2	1	L^3_2	1	L^5_2	L^6_2
W_m	L^1_6	L^2_6	L^3_6	L^4_6	1	1

Таблица 5 Матрица сравнения L

При помощи программы – измерителя снимаются с маршрутизирующих устройств необходимые пути передачи данных вида (Ui → Uq→ … → Ur→ Uj) (рис.3) по сети-отправителю и сети-получателю, на пересечении которых L[i,j] = 0. На основании полученной матрицы сравнения выполняется построение графа G=(U,V), в котором критичные маршруты (где большинство L=0) выделяются цветом. Данные, полученные системой передаются для рассмотрения администратору безопасности. Выполняется переход к шагу 1.

Реализация данной модели представила модульную программную систему, реализованную в среде Java с использованием модулей, реализованных на языках Python и Bash, в совокупности полностью выполняющую функции разработанной системы АСОИн ИБ КСПД.

Эксперименты, проведенные с реализованной системой, позволили сделать выводы о том, что за минимальное время методом простейшего сканирования маршрутизирующего оборудования КСПД можно обнаружить факты возникновения инцидентов ИБ в сети, и выделить самые критичные зоны воздействия инцидента, и зоны, попавшие в область воздействия.

Время работы программы не составляет более 15 секунд, время обработки данных составляет не более 5 минут. Режим запуска программы в КСПД подразумевается 2 раза в 1 час, однако в связи с тем, что программа ведет последовательный опрос оборудования, никакой дополнительной нагрузки на сетевые каналы она не несет, что позволяет выполнять подобное сканирование КСПД круглосуточно, получая данные о вероятных инцидентах ИБ по требованию администратора ИБ, либо при выполнении определенных настроек – ПО имеет функционал самостоятельно сигнализировать на АРМ администратора ИБ о вероятном инциденте ИБ.

Таким образом, можно сделать вывод о возможности внедрения разработанного программного продукта на КСПД современных предприятий как дополнительный инструмент обеспечения ИБ администратору безопасности предприятия.

Литература

1. Технологии для "зеленой" экономики. / Сайт Российского Национального комитета содействия Программе ООН по окружающей среде (ЮНЕПКОМ). URL: http://www.unepcom.ru/unep/gei/214-green-course.html.
2. Irina Makarova, Rifat Khabibullin, Eduard Belyaev, Dmitry Zhdanov. Intellectualization of transport systems for the benefit of safety and the sustainable development of territories. // Journal of International Scientific Publications: Ecology&Safety, Vol. 7, Part 3. Bulgaria. – 2013. P. 189-199. http://www.scientific-publications.net/ download/ecology-and-safety-2013-3.pdf
3. Irina Makarova, Rifat Khabibullin, Eduard Belyaev and Vadim Mavrin Increase of City Transport System Management Efficiency with Application of Modeling Methods and Data Intellectual Analysis // Intelligent Transportation Systems – Problems and Perspectives, Springer International Publishing AG Switzerland is part of Springer Science+Business Media. 2015, P. 37-80
4. Федоров, С.В. Совершенствование методов проектирования транспортных сетей и маршрутных систем крупных городов: автореф. дис. канд. техн. наук. - МАДИ, 2011. – 20 с.
5. Деловая электронная газета Татарстана. URL: http://www.business-gazeta.ru/article/55907/.
6. Генеральный план г.Набережные Челны: Материалы по обоснованию проекта. Пояснительная записка, т. 3. - Казань: 2009. - 140 с.
7. Генеральный план г.Набережные Челны: Материалы по обоснованию проекта. Пояснительная записка, т. 9. - Казань: 2009. -12с.
8. Михайлов А.Ю. Современные кольцевые пересечния, Иркутск: 2009. -103с.