МОНИТОРИНГ ИНФОРМАЦИОННО-ТЕЛЕКОММУНКАЦИОННЫХ СЕТЕЙ

Д.А. Груздев, П.В. Закалкин, С.И. Кузнецов, С.П. Тесля

Одной из первоочередных задач по обеспечению информационной безопасности информационно-телекоммуникационных сетей связи специального назначения является создание динамической системы защиты информации, позволяющей оперативно адаптироваться под быстро изменяющиеся условия функционирования объекта защиты. Необходимым условием реализации динамических систем защиты является наличие эффективной системы мониторинга.

Ключевые слова: информационная безопасность, мониторинг, сети связи специального назначения.

MONITORING OF INFORMATION AND TELEKOMMUNKATSIONNY NETWORKS

Gruzdev D., Zakalkin P., Kuznetsov S., Teslya S.

One of priorities on ensuring information security of information and telecommunication communication networks of a special purpose is creation of dynamic system of the information security allowing to adapt quickly under quickly changing operating conditions of object of protection. A necessary condition of realization of dynamic systems of protection is existence of effective system of monitoring.

Keywords: information security, monitoring, communication networks of a special purpose.

Одной из первоочередных задач по обеспечению информационной безопасности (ИБ) является создание динамической системы защиты информации, позволяющей оперативно адаптироваться под быстро изменяющиеся условия функционирования объекта защиты [1, 2].

При этом необходимым условием реализации динамических систем защиты является наличие эффективной системы мониторинга, которая выявит:

1) потенциальные уязвимости информационно-телекоммуникационных сетей (ИТКС);

2) нарушения в порядке реализации установленных процедур.

В настоящее время для термина «мониторинг» существует ряд определений.

В статье под мониторингом понимается любая деятельность по выявлению ключевых (явных или косвенных) признаков (параметров) объектов мониторинга, влияющих на уровень защищенности информационно-телекоммуникационных сетей связи.

Процесс мониторинга распределен во времени и должен охватывать:

1) состояния объекта мониторинга в прошлом (например, SIEM системы по сохраненным ранение журналам событий от различных источников сетевых устройств, приложений, журналов ОС и др.);

2) текущие состояния объекта мониторинга (сбор и анализ информации о функционировании и состоянии объекта контроля в настоящее время);

3) состояния объекта мониторинга в будущем времени (по прошлым и текущим состояниям объекта мониторинга прогнозируется его дальнейшее состояние и адаптация к изменившимся условиям функционирования, т. е. принимаются оптимизирующие управленческие решения).

Можно выделить совокупность требований, предъявляемых к мониторингу:

1) своевременность (обнаружение (предсказание) факта перехода объекта мониторинга в предельные состояния);

2) полнота (достаточность данных для определения требуемых свойств объекта мониторинга);

3) достоверность (мониторинг должен отражать истинное состояние ОМ объекта мониторинга);

4) целенаправленность (направленность на достижение определенного конечного результата, использование типа мониторинга, позволяющего наиболее корректно и точно выполнять возложенные на него задачи);

5) объективность (вывод о параметрах поведения/состояния объекта мониторинга не должен зависеть от воли или желания человека);

6) гибкость (возможность адаптации к происходящим изменениям).

Однако, это требования в некоторых моментах противоречивы и при упоре на одно из них, мы получим ухудшение параметров других. Так, к примеру, повышая достоверность мониторинга, мы вынуждены повышать и его полноту, но при этом повышается объем входящих данных и увеличивается время, необходимое на обработку и анализ. Соответственно, говорить о таком требовании как «своевременность» уже не приходится. При всём этом, мы не можем сказать, насколько система мониторинга должна быть гибкой, чтобы оптимально расставить приоритеты для заданной совокупности требований.

Для обеспечения оптимального функционирования ИТКС необходимо осуществлять мониторинг на всех временных этапах их функционирования.

При этом задача мониторинга ИТКС усложняется тем, что:

1) необходимо контролировать большое количество параметров как элементов ИТКС, так и системы в целом;

2) все элементы ИТКС являются неравнозначными;

3) деструктивные воздействия могут быть осуществлены из любой точки на любую точку в границах ИТКС;

4) воздействия являются результатом учета значительного числа факторов;

5) существует устойчивая тенденция роста приоритета методов временного снижения свойств элементов ИТКС над методами безвозвратного их уничтожения;

6) силы и средства мониторинга ограничены [3].

В этих условиях становится актуальной задача определения оптимального количества контролируемых параметров, что позволит минимизировать расход

сил и средств мониторинга (измерений) и сохранить заданный уровень информированности о состоянии объекта мониторинга.

Для решения задачи предлагается способ, реализация которого поясняется блок-схемой алгоритма, представленного на рисунке.

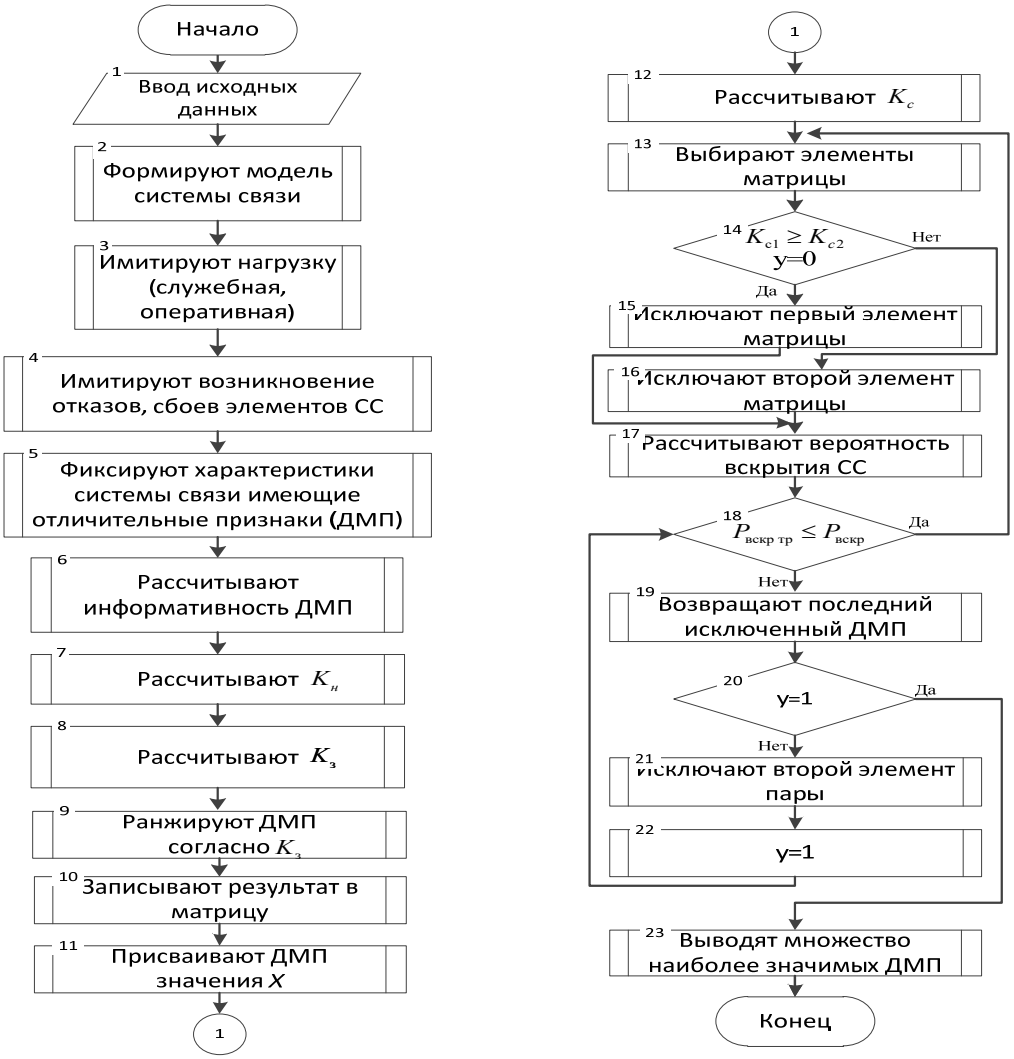

Рисунок. Блок-схема алгоритма выбора минимального множества контролируемых параметров

Исходными данными для алгоритма являются:

1) заданные значения вероятностей: обнаружения демаскирующих признаков (ДМП) элементов системы связи $P_{обн}$ и распознавания ДМП элементов системы связи $P_{расп}$;

2) данные о системе связи: состав, структура системы связи; матрица связности системы связи; матрица маршрутизации; матрица приоритетов сообщений, передаваемых по системе связи;

3) вероятности появления характерных ДМП элементов системы связи;

4) требуемая вероятность вскрытия элемента системы связи $P_{вскр}$;

5) задается стоимость всех потенциально возможных каналов измерения X.

Далее происходит формирование модели системы с характерными демаскирующими признаками ее элементов. Формирование модели системы связи является известной процедурой и проводится по правилам, изложенным в [4, 5, 6].

Имитируется служебная и оперативная нагрузки, а также возникновение эксплуатационных отказов, сбоев программного обеспечения, техногенных повреждений, перемещения элементов системы связи, факторов природного воздействия, деструктивных программных воздействий и появление на их основе ДМП.

Рассчитывают информативность полученных ДМП. Расчет информативности описан в [7].

Рассчитывают долю времени, в течение которого ДМП доступен средствам контроля (разведки) $K_н$.

Под коэффициентом исправного действия понимается отношение среднего времени исправной работы к общему времени функционирования системы.

Учитывая, что частота проявления и время существования являются величинами определяющими временные характеристики ДМП, а $T_{\text{контроля}}$ – характеристика, относящаяся к времени контроля, то по аналогии с коэффициентом полезного действия возможно свернуть частные временные показатели [8]:

а) коэффициент наблюдаемости ДМП $K_{\text{н}}$:

$$K_{\text{н}} = \frac{\bar{n}_{\text{проявл ДМП}} \cdot \bar{t}_{\text{сущ ДМП}}}{T_{\text{контроля}}},$$

где $\bar{t}_{\text{сущ ДМП}}$ – среднее время существования ДМП при каждом проявлении; $\bar{n}_{\text{проявл ДМП}}$ – среднее количество проявлений ДМП; $T_{\text{контроля}}$ – общее время контроля ДМП;

б) коэффициент значимости ДМП $K_{\text{з}}$:

$$K_{\text{з}} = K_{\text{н}} \cdot K_{\text{инф}},$$

где $K_{\text{н}}$ – коэффициент наблюдаемости ДМП; $K_{\text{инф}}$ – информативность ДМП;

в) относительную стоимость создания канала измерения *i*-го ДМП $K_{\text{с}}$:

$$K_{\text{с}} = \frac{X_i}{X_{max}}, \quad i = \{1,2, \dots, N\},$$

где X_i – стоимость создания канала измерения *i*-го ДМП; X_{max} – максимальная стоимость создания канала измерения для зафиксированных ДМП.

Далее ДМП ранжируют согласно $K_{\text{з}}$ по возрастанию от минимального значения до максимального.

Записывают полученные значения в матрицу *I* размером (1x*N*), где *N* – общее количество зафиксированных ДМП.

Присваивают каждому зафиксированному ДМП значение стоимости создания канала измерения *X* согласно исходных данных.

В соответствии с заданными правилами (бл. 14–22, рис.) проводят ранжирование ДМП.

Выходными данными является минимальное множество наиболее информативных ДМП, необходимых для оптимального функционирования системы мониторинга.

Таким образом, в результате применяемого способа будет сокращено количество контролируемых системой мониторинга параметров (ДМП), что позволяет минимизировать использование сил и средств мониторинга (измерений) и сохранить заданный уровень информированности о состоянии объекта мониторинга.

Список используемых источников

1. Стародубцев Ю. И., Евграфов А. А., Сухорукова Е. В. Проблема формирования системы показателей для оценки защищенности информационно-телекоммуникационных сетей // Проблемы экономики и управления в торговле и промышленности. 2014. № 3. С. 80–86.

2. Коцыняк М. А., Лаута О. С., Осадчий С. А. Методика оценки устойчивости интегрированной информационно-телекоммуникационной сети в условиях компьютерных атак // Информация и космос. 2014. № 2. С. 38–41.

3. Стародубцев Ю. И., Сухорукова Е. В., Чукариков А. Г. Методика выявления критически важных элементов информационно-телекоммуникационных систем // Проблемы экономики и управления в торговле и промышленности. 2014. № 1 (5). С. 95–101.

4. Иванов Е. В. Имитационное моделирование средств и комплексов связи и автоматизации. СПб.: ВАС, 1992. 206 с.

5. Сухорукова Е. В., Закалкин П. В., Андреянов С. Н. Моделирование торговых бизнес-процессов: способы задания модельного времени // Проблемы экономики и управления в торговле и промышленности. 2013. № 1. С. 104–109.

6. Стародубцев Ю. И., Сухорукова Е. В., Закалкин П. В., Стекольщикова Г. А. Способ адаптивного повышения адекватности модели информационно-телекоммуникационной системы // Проблемы экономики и управления в торговле и промышленности. 2015. № 2 (10). С. 94–100.

7. Пат. 2459370 Российская Федерация, МПК H04L 12/00. Способ построения защищенной системы связи» / Белов А.С., Иванов В.А., Стародубцев Ю.И. и др. (РФ); заявитель Академия ФСО России, заявл. 28.06.10 ; опубл. 20.08.12, Бюл. № 23. 13 с., илл.

8. Заявка 2014111877/08 Российская Федерация, МПК G01R 29/08, G06N 5/00. Способ выбора минимального множества демаскирующих признаков, необходимого для идентификации объекта с данной достоверностью / Алисевич Е.А., Закалкин П.В., Стародубцев Ю.И., Сухорукова Е.В. (РФ); заявитель СПбГТЭУ, заявл. 27.03.2014, опубл. 10.10.2015, Бюл. № 28. 5 с., илл.