УДК 004.056 Вестник УрФО № 4(18) / 2015, стр. 4–11

Агафонов А. В., Синадский Н. И.

СТРУКТУРА И ПРИНЦИП РАБОТЫ КОМПЛЕКСА ТЕСТИРОВАНИЯ УСТОЙЧИВОСТИ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ К СЕТЕВЫМ АТАКАМ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

В статье рассмотрены структура и принцип работы аппаратно-программного комплекса, предназначенного для тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании». Для тестирования в комплексе используется сетевой трафик, генерируемый на основе модели сетевой среды функционирования телекоммуникационного оборудования, оптимальные значения параметров которой определяются в процессе тестирования генетическим алгоритмом.

В статье также приведены алгоритмы, используемые для вычисления характеристик, связанных с искажениями межпакетных интервалов и потерей пакетов тестового сетевого трафика в процессе его обработки тестируемым образцом.

Ключевые слова: *тестирование, телекоммуникационное оборудование, отказ в обслуживании, генетический алгоритм, комплекс.*

Agafonov A., Sinadsky N.

STRUCTURE AND OPERATION PRINCIPLE OF THE HARDWARE AND SOFTWARE COMPLEX INTENDED FOR TESTING THE IMMUNITY OF TELECOMMUNICATION EQUIPMENT AGAINST DENIAL OF SERVICE NETWORK ATTACKS

The article describes the structure and operation principle of the hardware and software complex intended for testing the immunity of telecommunication equipment against denial of

service network attacks. Network traffic used for testing is generated by the model of telecommunications equipment network environment, which parameters optimal values are determined by the genetic algorithm during the testing process. The article also describes the algorithms used to calculate characteristics related to the inter-packets intervals distortion and packet loss of the test network traffic appears during its processing.

Keywords: *testing, telecommunications equipment, denial of service, genetic algorithm, complex.*

Введение

В условиях построения в Российской Федерации информационного общества и формирования глобального информационного пространства подавляющее большинство систем принятия решений и управления в ключевых областях экономики и государственного управления создается с использованием современных информационных технологий. В частности, в различных отраслях промышленности получили распространение автоматизированные системы управления технологическими процессами (АСУ ТП), которые за счет автоматизации процессов управления технологическим оборудованием повышают эффективность производственных процессов.

АСУ ТП представляет собой сложную распределенную автоматизированную систему, отдельные элементы которой объединены с помощью управляющей компьютерной сети, являющейся совокупностью линий связи и телекоммуникационного оборудования (ТКО) [1].

Вывод из строя ТКО управляющей сети может привести как к существенным задержкам передачи данных и их потерям, так и к полному прекращению информационного взаимодействия между узлами сети, и, таким образом, приведет к нарушению структурной целостности всей АСУ ТП. Поэтому для злоумышленника, стремящегося нарушить штатное выполнение технологического процесса, наиболее выгодным для атаки элементом является именно ТКО.

Распространенным способом вывода его из строя являются компьютерные атаки типа «отказ в обслуживании», реализуемые путем использования ошибок в реализациях сетевых протоколов, а также в программном и аппаратном обеспечении. Данные ошибки приводят к некорректной обработке атакующего сетевого трафика и вызывают критическую нагрузку на процессоры и оперативную память ТКО, в результате чего резко увеличиваются задержки передачи данных в сети.

Сложность оценки защищенности АСУ ТП от указанного типа атак заключается в том, что их управляющие сети в типовой конфигурации построены, как правило, на базе коммутаторов и машрутизаторов иностранного производства, в частности фирм Cisco Systems, Siemens и MOXA, для которых недоступны исходные программные коды встроенного программного обеспечения, что на практике приводит к невозможности его анализа для поиска скрытых уязвимостей.

С другой стороны, существующие методики тестирования ТКО [2, 3], не требующие информации о внутреннем устройстве тестируемых образцов и используемые при проведении сертификационных испытаний и мероприятий по анализу уязвимостей [1], не позволяет в полной мере воспроизводить в процессе тестирования условия, существующие при проведении атак такого типа, что снижает, в конечном счете, достоверность результатов мероприятий по анализу уязвимостей АСУ ТП в целом.

Таким образом, возникает потребность в повышении эффективности обнаружения уязвимостей ТКО к данному классу атак, которая может быть реализована путем создания практического инструмента тестирования ТКО, позволяющего более точно воспроизводить условия проведения атак типа «отказ в обслуживании».

На сегодняшний день существует множество разновидностей ТКО, обеспечивающих функционирование компьютерных сетей различных типов. Разработанный авторами комплекс предназначен для тестирования маршрутизаторов IP и коммутаторов Ethernet, однако использованные подходы также могут быть применены при создании средств тестирования ТКО других типов.

Структура аппаратно-программного комплекса

При разработке аппаратно-программного комплекса тестирования устойчивости ТКО к атакам типа «отказ в обслуживании» был решен ряд задач:

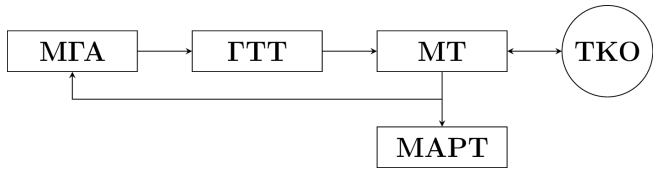

Рис. 1. Структура комплекса тестирования ТКО

1. Воспроизведение тестового сетевого трафика (СТ) и одновременная запись СТ, полученного после обработки тестируемого устройства с сохранением временных отметок сетевых пакетов. Данную задачу в составе комплекса решает модуль тестирования (МТ).

2. Генерация тестового СТ, обладающего заданными параметрами. Данную задачу решает генератор тестового трафика (ГТТ) на основе параметрической модели сетевой среды функционирования (ССФ) ТКО4.

3. Поиск таких сочетаний параметров СТ, при которых потери пакетов и искажения межпакетных временных интервалов, возникающих в СТ при его обработке тестируемым устройством, оказываются наибольшими. Задача решена на основе аппарата генетических алгоритмов (ГА)5 и реализована в модуле генетического алгоритма (МГА).

4. Определение границ областей пространства параметров СТ, где потери пакетов и искажения межпакетных временных интервалов в СТ, обрабатываемого тестируемым устройством, оказываются больше заданного предельно допустимого значения. Данную задачу решает модуль анализа результатов тестирования (МАРТ).

Таким образом, разработанный комплекс представляет собой тестовый стенд, структура которого приведена на рис. 1, где ТКО — тестируемый образец телекоммуникационного оборудования.

Процедура тестирования реализуется следующим алгоритмом:

1. Создать с помощью МГА начальную популяцию $\{M_j\}_{j=\overline{1,m}}$, содержащую случайным образом сгенерированные совокупности значений параметров модели ССФ ТКО.

2. Цикл $i := \overline{1,n}$, где n — количество итераций генетического алгоритма:

2.1. Цикл $j := \overline{1,m}$:

2.1.1. С помощью ГТТ сгенерировать тестовый СТ на основе особи M_j.

2.1.2. С помощью МТ произвести тестирование ТКО с использованием тестового СТ.

2.1.3. С помощью МТ определить результаты тестирования, выраженные численными значениями искажений СТ при его обработке ТКО, и вместе с параметрами M_j передать их МАРТ и МГА.

2.2. Произвести с помощью МГА селекцию популяции на основе полученных результатов тестирования.

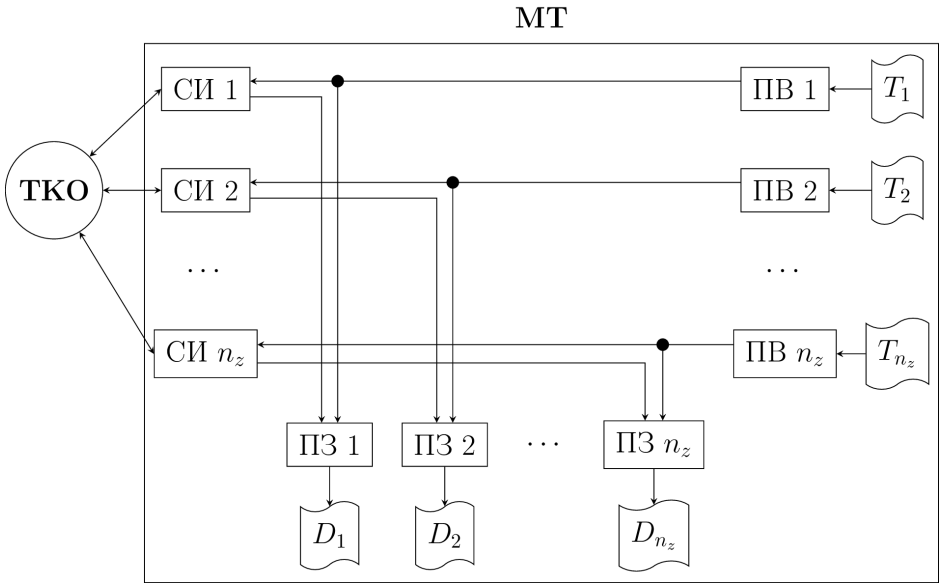

Рис. 2. Структура модуля тестирования

3. С помощью МАРТ на основе множества сохраненных результатов тестирования найти области пространства параметров модели ССФ ТКО, где задержки передачи СТ, обрабатываемого тестируемым устройством, оказались неудовлетворительными.

Принцип работы модуля тестирования

В процессе работы модуля тестирования, схема которого представлена на рис. 2, сформированные массивы тестового СТ $\{T_j\}_{j=1}^{z}$ передаются для воспроизведения сетевыми интерфейсами (СИ) МТ программами воспроизведения (ПВ).

Одновременно на всех СИ МТ программами записи (ПЗ) производится сохранение пакетов, как отправляемых, так и принимаемых с СИ, в соответствующие файлы $\{D_j\}_{j=1}^{n_z}$.

Для количественной оценки потерь пакетов и искажений межпакетных интервалов в тестовом СТ, которые возникают при его обработке ТКО, необходимо определить соответствие между отправленными и принятыми пакетами, содержащимися в данных файлах.

Схема, описывающая процедуру выделения в файлах СТ последовательности пар пакетов, приведена на рис. 3.

Шаг 1 заключается в разделении массивов $\{D_j\}_{j=1}^{n_z}$ на очереди, содержащие пакеты, отправленные с i-го СИ и захваченные в моменты их отправки МТ (S_i) и приема после обработки ТКО (R_i).

Шаг 2 реализует сопоставление пакетов, содержащихся в S_i, пакетам R_i. Для корректной обработки случаев, связанных с нарушением порядка следования отправленных и принятых пакетов, а также потерь пакетов, применяются двумерные массивы $\{B_i\}_{i=1}^{n_z}$, хранящие отправленные и соответствующие им принятые пакеты. Данные массивы имеют следующую структуру:

$$B_i = \begin{pmatrix} b_{i,1,s} & b_{i,2,s} & \cdots & b_{i,l,s} \\ b_{i,1,r} & b_{i,2,r} & \cdots & b_{i,l,s} \end{pmatrix}$$

где l — длина буфера. В j-м столбце массива содержится пара пакетов $\langle b_{i,j,s}, b_{i,j,r} \rangle$ соответственно отправленного с i-го СИ (обозначен индексом s) и принятого на каком-либо СИ МТ после обработки (обозначен индексом r), причем пакет $b_{i,j+1,s}$ является отправленным непосредственно после $b_{i,j,s}$.

В результате выполнения шага 2 формируются очереди $\{Y_i\}_{i=1}^{n_z}$ обнаруженных пар пакетов $\langle y_{i,j,s}, y_{i,j,r} \rangle$. Каждая из очередей Y_i по структуре аналогична массивам B_i, однако не имеет ограничения по длине и задается выражением:

$$Y_i = \begin{pmatrix} y_{i,1,s} & y_{i,2,s} & \cdots \\ y_{i,1,r} & y_{i,2,r} & \cdots \end{pmatrix}$$

Массивы $\{B_i\}_{i=1}^{n_z}$ инициализируются по следующему алгоритму:

1. Произвести чтение по l пакетов из каждого файла $\{S_i\}_{i=1}^{n_z}$ в массивы соответственно $\{\langle s_{i,1}, \cdots, s_{i,l} \rangle\}_{i=1}^{n_z}$.

2. Заполнить ячейки $\{B_i\}_{i=1}^{n_z}$ пакетами соответствующих массивов $\{\langle s_{i,1}, \cdots, s_{i,l} \rangle\}_{i=1}^{n_z}$: $b_{i,j,s} := s_{i,j}$, где $i = \overline{1,n_z}$, $j = \overline{1,l}$.

3. Обозначить ячейки принятых пакетов пустыми: $b_{i,j,r} := 0$, где $i := \overline{1,n_z}$, $j := \overline{1,l}$.

Также массивы $\{B_i\}_{i=1}^{n_z}$ поддерживают процедуру загрузки принятого пакета r, далее обозначенную как $load(B_i, r)$, которая имеет следующий алгоритм:

1. Определить значение $j \in \overline{1,l}$, такое что значение поля Identication [6] заголовка IP пакетов r и $b_{i,j,s}$ совпадают.

2. Если j не найдено, то завершить процедуру.

3. $b_{i,j,r} := r$.

4. Если $j < l/2$, то $n := 1$, иначе — $n := 2$.

5. Цикл, где $k := \overline{1,n}$:

5.1. Если $b_{i,l,r} \neq 0$, то добавить $\langle b_{i,l,s}, b_{i,l,r} \rangle$ в очередь пар пакетов Y_i.

5.2. $b_{i,j,s} := b_{i,j+1,s}$, $b_{i,j,r} := b_{i,j+1,r}$, где $i := \overline{1,z}$, $j := \overline{1,l-1}$.

5.3. Произвести чтение из S_i одного пакета в $b_{i,l,s}$.

5.4. $b_{i,l,r} = 0$.

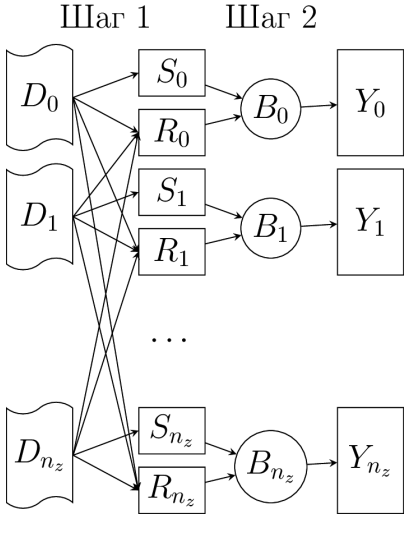

Рис. 3. Схема выделения в файлах СТ пар пакетов

Процедура определения соответствия между отправленными и принятыми пакетами имеет алгоритм:

1. Инициализировать $\{B_i\}_{i=1}^{z}$.

2. Произвести чтение по одному пакету из файлов $\{R_i\}_{i=1}^{z}$: $\{r_i\}_{i=1}^{z}$.

3. Цикл до прочтения всех пакетов из $\{R_i\}_{i=1}^{z}$:

3.1. Выбрать из $\{r_i\}_{i=1}^{z}$ пакет с минимальным значением времени приема: r_k.

3.2. Цикл, где $i=\overline{1,z}, j=\overline{1,l}$:

3.2.1. Если значение поля Identication заголовка IP пакетов r_k и $b_{i,j,s}$ совпадают:

3.2.1.1. Выполнить процедуру $load(B_i, r_k)$.

3.2.1.2. Произвести чтение из R_k одного пакета в r_k.

3.2.1.3. Прервать текущий цикл.

Для очередей пакетов Y_i вычисляются следующие временные характеристики:

– задержка передачи *i*-го пакета, $t_{d,i}$:

$$t_{d,i} = t_{r,i} - t_{s,i},$$

– разность межпакетных интервалов *i*-х отправленного и принятого пакетов, $t_{p,i}$:

$$t_{p,i} = (t_{r,i} - t_{r,i-1}) - (t_{s,i} - t_{s,i-1})$$

На основе данных характеристик отдельных пар пакетов вычисляются интегральные временные параметры массива в целом, определяющие потери пакетов и искажения межпакетных временных интервалов в тестовом СТ при его обработке ТКО и отражающие эффективность данного СТ как потенциальной реализации атаки типа «отказ в обслуживании»:

– средняя задержка передачи пакетов, $\overline{t_d}$:

$$\overline{t_d} = \frac{\sum_{i=1}^{n} t_{d,i}}{n}$$

– средняя разность межпакетных интервалов отправленных и принятых пакетов, $\overline{t_p}$:

$$\overline{t_p} = \frac{\sum_{i=1}^{n} t_{p,i}}{n}$$

– среднеквадратическое отклонение разности межпакетных интервалов отправленных и принятых пакетов, называемое также джиттером [7], $\sigma(t_p)$:

$$\sigma(t_p) = \sqrt{\frac{\sum_{i=1}^{n} (t_{p,i} - \mu(t_p))^2}{n}}$$

– относительная доля потерь пакетов *q*:

$$q = \frac{m-n}{m}$$

где *m* — количество пакетов тестового СТ, отправленных тестируемому образцу ТКО, а *n* — количество пакетов тестового СТ, принятых МТ после их обработки данным образцом. При этом учитываются лишь пакеты, которые были корректно отправлены ТКО с тех СИ, где узлы – получатели пакетов считаются доступными в соответствии с моделируемой топологией сети.

Результатом работы модуля тестирования является журнал тестирования — файл, содержащий соответствия между значениями параметров модели ССФ ТКО, использованными в процессе тестирования и вычисленными в результате значениями $\overline{t_d}$, $\overline{t_p}$, $\sigma(t_p)$, и *q* для СТ, сгенерированного на основе параметров модели. Данный файл передается для дальнейшей обработки МАРТ и МГА.

Принцип работы генератора тестового трафика

Принцип работы ГТТ основан на использовании для генерации файлов, содержащих образцы тестового СТ, значений параметров модели ССФ ТКО, позволяющей производить имитацию условий внешней среды, в которой функционирует тестируемый образец ТКО. Под условиями внешней среды в данном случае понимается совокупность структуры компьютерной сети, в которую образец включен, и статистических характеристик обрабатываемого им сетевого трафика (как штатного, так и содержащего атакующее воздействие).

Модель M задается выражением:

$$M = \left\langle H, W, Z, f_{wz}, \left\langle G_i \right\rangle_{i=1}^{n_g}, f_g \right\rangle$$

где использованы следующие обозначения:

– $H = \{\overline{1, n_h}\}$ — множество узлов сетей, где n_h — их количество;

– $W = \{w_i \subseteq H\}_{i=1}^{n_w} : (\forall w_i, w_j \in W : w_i \cap w_j = \varnothing)$ – множество сетей,

где n_z — их количество;

– $Z = \{z_i \subseteq W\}_{i=1}^{n_z}$ — множество сетевых интерфейсов (СИ) ТКО,

где n_z — их количество;

– $\left\langle G_i \right\rangle_{i=1}^{n_g}$ — массив групп потоков;

– F_g — функция распределения (ФР) [8] вероятности события генерации в СТ потока каждой из n_g групп G_i.

Под термином «поток» в данном случае подразумевается множество пакетов, создаваемых в процессе двунаправленного обмена данными между двумя конечными узлами сети с использованием протоколов транспортного уровня или управления сетью в течение определенного интервала времени.

Группа потоков G_i — множество потоков, имеющих идентичные значения следующих параметров, характеризующих логическое соединение между взаимодействующими сетевыми узлами: идентификатора типа потока a, определяющего как используемый протокол транспортного уровня или управления сетью, так и наличие в потоке атакующего воздействия определенного типа; сетевых адресов: узла – инициатора процесса передачи данных (УИ) $h_1 \in H$ и узла, взаимодействующего с инициатором (УВ), $h_2 \in H$; номеров портов (для протоколов транспортного уровня) или типов генерируемых сообщений (для протоколов управления сетью) УИ p_1 и УВ — p_2.

При этом для каждой из групп G_i определены статистические характеристики СТ, связанные с размером и распределением сетевых пакетов во времени и заданные своими ФР, которые сгруппированы в векторы:

– $C_0 = \langle F_h, F_f \rangle$ — вектор характеристик, не связанных с направлениями передачи данных, где F_h — ФР вероятности события генерации трафика конечными узлами группы потоков, а F_f — ФР длительности потока внутри группы;

– $C_1 = \langle F_{l1}, F_{t1} \rangle$, $C_2 = \langle F_{l2}, F_{t2} \rangle$ — вектор характеристик, связанных с направлениями передачи соответственно от УИ к УВ и от УВ к УИ, где F_{li} — ФР размера пакета, F_{ti} — ФР промежутка времени между началами передач двух последовательных пакетов.

Алгоритм генерации тестового СТ на основе значений параметров модели ССФ ТКО подразумевает выполнение следующих шагов:

1. Определить на основе значения параметра F_g модели ССФ ТКО для каждого i-го из n генерируемых потоков группу G_i, к которой он относится, и момент времени $t_{0,i}$ его начала.

2. Для каждого из генерируемых потоков на основе значения параметра F_f соответствующей группы G_i определить момент времени завершения потока $t_{1,i}$.

3. Произвести преобразование индексов узлов h_1, h_2 каждой из групп G_i в IP-адреса сетей, соответствующих значениям множества W модели.

4. В зависимости от значения параметра a выбрать алгоритм генерации СТ потока соответствующего типа (TCP, UDP или ICMP).

5. Цикл для $i := \overline{1, n}$:

5.1. Сгенерировать последовательности пакетов потоков.

5.2. Упорядочить пакеты по времени.

5.3. В зависимости от точки подключения $z_j \in Z$ узла-отправителя каждого из пакетов к ТКО распределить их по файлам $\{T_j\}_{j=1}^{n_z}$.

6. Промаркировать пакеты путем записи в поле Identication заголовка IP каждого из пакетов файлов $\{T_j\}_{j=1}^{n_z}$ номера СИ ТКО z и порядкового номера пакета для возможности его идентификации и дальнейшего вычисления задержки передачи.

Принцип работы модуля генетического алгоритма

МГА реализует процедуру поиска критических условий внешней среды на основе ГА, моделирующего механизмы биологической эволюции, то есть чередования поколений популяции, включающего этапы размножения, мутагенеза и селекции. При этом особи, составляющие популяцию в реализованном алгоритме, представляют собой совокупность внутренних параметров, соответствующих содержанию модели ССФ ТКО, и внешних, отражающих результаты тестирования образца ТКО с использованием сетевого трафика, сгенерированного на основе внутренних:

– средней задержки передачи пакетов, $\overline{t_d}$;

– среднего значения $\overline{t_p}$ и дисперсии $\sigma(t_p)$ отклонения межпакетного интервала принятых пакетов от изначального;

– относительной доли q пакетов, потерянных в процессе тестирования.

В процессе выполнения генетического алгоритма параметры особей изменяются таким образом, что каждое последующее поколение показывает в сравнении с предыдущим неменьшее среднее значение указанных внешних параметров.

Принцип работы модуля анализа результатов тестирования

Для обнаружения критических областей на основе журнала тестирования используется модуль анализа результатов тестирования, принцип работы которого заключается в кластерном анализе особей последнего поколения ГА. При этом особи рассматриваются как точки факторного пространства, образуемого их параметрами.

На предварительном этапе производится нормализация координат точек путем их деления на значение их среднеквадратического отклонения по популяции по соответствующим осям. Нормализация является необхо-

димой для приведения разнородных координат пространства параметров особей к единой безразмерной величине.

Поведение алгоритма кластеризации определяется сочетанием способов вычисления расстояний между кластеризуемыми объектами, а также направлением кластеризации.

Дистанция d между i-й и j-й особями в данном случае определяется как евклидово расстояние между соответствующими им точками k-мерного нормализованного факторного пространства. При вычислении же расстояний между кластерами используется метод взвешенного попарного среднего, где в качестве весового коэффициента используется размер соответствующих кластеров, то есть число объектов, содержащихся в них.

Кластеризация производится иерархически в направлении «снизу – вверх». При этом выделяются кластеры, для которых значения внешних параметров особей больше предельно допустимых значений искажений сетевого трафика при его обработке ТКО, которые задаются пользователем комплекса. Для выделенных таким образом кластеров производится вычисление математического ожидания и дисперсии по каждой из осей координат, что позволяет определить местоположение и форму искомых областей, где наблюдаются недопустимо сильные искажения временных параметров СТ, обрабатываемого тестируемым устройством.

Заключение

Разработанный комплекс позволяет моделировать сетевую среду функционирования ТКО и производить поиск таких сочетаний параметров данной среды, при которых тестируемое ТКО оказывается неспособно обеспечить уровень искажений обрабатываемого сетевого трафика на допустимом уровне. При этом для работы комплекса не требуется наличие исходных программных кодов встроенного программного обеспечения тестируемого устройства, которое рассматривается как «черный ящик».

С помощью комплекса был протестирован коммутатор MOXA EDS 408A PN, применяющийся в составе типовой конфигурации АСУ ТП.

В результате были обнаружены сочетания параметров СТ, при которых значительно возрастают (в сравнении со штатным режимом функционирования) потери пакетов, задержки передачи данных и джиттер, возникающие в данном СТ при его обработке ТКО. Данная ситуация может привести к нарушениям функционирования приложений АСУ ТП, требующих передачи данных в реальном масштабе времени.

Таким образом, предложенный подход позволяет выявить уязвимости ТКО, применяемого для построения АСУ ТП, к компьютерным атакам типа «отказ в обслуживании», и, следовательно, предупреждает возможности атакующего воздействия на технологическую инфраструктуру предприятий промышленности.

Примечания

1. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

2. McQuaid S., Bradner J. IETF RFC 2544: Benchmarking methodology for network interconnect devices. URL: http://www.ietf.org/rfc/rfc2544.txt (дата обращения: 25.11.2015).

3. Stopp D., Hickman B. IETF RFC 3918: IP Multicast Throughput No Drop Rate Test. URL: http://www.ietf.org/rfc/rfc3918.txt (дата обращения: 25.11.2015).

4. Агафонов А. В. Выделение структурных элементов сетевого трафика реальных сетей в задаче тестирования коммуникационного оборудования // Безопасность информационного пространства : Материалы XII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых (Екатеринбург, 2-4 декабря 2013 года) / под ред. В. В. Бакланова, А. С. Лучинина, М. П. Трухина. — Екатеринбург : Изд-во Урал. ун-та, 2014. — С. 103–109.

5. Goldberg D. E. Genetic Algorithms in Search, Optimization, and Machine learning. — Boston : Addison-Wesley, 1989. — 432 p.

6. Postel J. IETF RFC 791: Internet Protocol. URL: http://www.ietf.org/rfc/rfc791.txt (дата обращения: 25.11.2015).

7. Shulzrinne H., Casner S., Frederick R., Jacobson V. IETF RFC 3550: RTP: A Transport Protocol for Real-Time Applications. URL: http://www.ietf.org/rfc/rfc3550.txt (дата обращения: 25.11.2015).

8. Вентцель Е. С. Теория вероятностей. — М. : Наука, 1969. — 576 с.

Алексей Владимирович Агафонов, аспирант кафедры Теоретических основ радиотехники, Институт радиоэлектроники и информационных технологий Уральского федерального университета им. первого Президента России Б. Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: avagaf@gmail.com

Николай Игоревич Синадский, к. т. н., доцент, доцент кафедры Теоретических основ радиотехники, Институт радиоэлектроники и информационных технологий Уральского федерального университета им. первого Президента России Б. Н. Ельцина; 620002, г. Екатеринбург, ул. Мира, 19. E-mail: nickis@e1.ru

Alexey Agafonov, postgraduate student, Department of Theoretical Foundations of Radio Engineering, Institute of Radioelectronics and Information Technologies,, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Russian Federation, Yekaterinburg, Mira str., 19. E-mail: avagaf@gmail.com

Nikolay Sinadsky, candidate of technical sciences, associate Professor, Department of Theoretical Foundations of Radio Engineering, Institute of Radioelectronics and Information Technologies, Ural Federal University named after first President of Russia B.N. Yeltsin; 620002, Russian Federation, Yekaterinburg, Mira str., 19. E-mail: nickis@e1.ru