УДК 004.414.23

**МОДЕЛИРОВАНИЕ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ПРОГРАММНО-АППАРАТНЫХ ВОЗДЕЙСТВИЙ**

Исупов Антон Борисович
*Военная академия связи (филиал г.Краснодар), Краснодар, Россия*

В статье рассмотрена модель процесса функционирования информационно-телекоммуникационной сети в условиях трех основных этапов типового программно-аппаратного воздействия (ПАВ). Определены параметры, влияющие на качество процесса обнаружения ПАВ

Ключевые слова: ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ, ПРОГРАММНО-АППАРАТНЫЕ ВОЗДЕЙСТВИЯ, НЕЧЕТКИЕ СЕТИ ПЕТРИ

UDC 004.414.23

**MODELING OF THE PROCESS OF FUNCTIONING OF THE TELECOMMUNICATION NETWORK UNDER SOFTWARE AND HARDWARE IMPACTS**

Isupov Anton Borisovitch
*Military academy of communication corps (Krasnodar branch office), Krasnodar, Russia*

The model of functioning of the telecommunication network in the conditions of three main stages of typical software and hardware impact is considered in the article. The factors, affecting the quality of the detection of software and hardware impacts are determined

Keywords: TELECOMMUNICATION NETWORKS, SOFTWARE AND HARDWARE IMPACTS, FUZZY PETRI NETS

В связи с интенсивной информатизацией и цифровизацией процессов управления [4] приоритетными становятся исследования в области информационного противоборства, в том числе устойчивости функционирования информационно-телекоммуникационных сетей (ИТС) в условиях программно-аппаратных воздействий (ПАВ).

Локальные вооруженные конфликты последнего десятилетия, в котором участвовали ВС США и страны блока НАТО, сопровождались активной отработкой технологий информационного противоборства. Так, конфликтам в Югославии, Афганистане, Ираке и Ливии предшествовало мощное информационно-психологическое воздействие как на сознание высшего военно-политического руководства, так и, прежде всего, на общественное мнение населения своей страны и мира, особенно, атакуемых государств. При дальнейшей эскалации конфликтов для поражения информационно-телекоммуникационных сетей государственного и военного управления активно применялись

радиоэлектронные и программно-аппаратные воздействия (компьютерные атаки).

В настоящее время информационное противоборство в ВС США и странах-участницах блока НАТО стало составной частью боевых действий, а в некоторых акциях их самостоятельной формой. В концепции «Единая перспектива-2020» ВС США подчеркивается, что главной чертой вооруженной борьбы в следующем столетии будет перенос акцента в сферу информационного противоборства, а приоритетной задачей ВС США на ближайшие 20 лет – достижение информационного превосходства над противником. С целью достижения информационного превосходства над противником в США и странах блока НАТО ведутся интенсивные исследования по разработке образцов вооружения нового поколения – информационного оружия, а также способов его применения и обеспечения защиты собственных ИТС в условиях ПАВ. Одними из перспективных видов информационного оружия являются средства реализации ПАВ на ИТС, которые в мирное время отрабатываются на информационно-телекоммуникационных сетях гражданского назначения.

По данным исследований, проведенных компанией InfoWatch и рядом зарубежных аналитических центров, в период с 2007 по 2010 гг. зафиксирован значительный рост числа отечественных и зарубежных информационно-телекоммуникационных сетей (ИТС), подвергшихся программно-аппаратным воздействиям. Согласно отчету CCIPS (Computer Crime and Intellectual Property Section) Министерства юстиции США за 2010 год [5] в период с 2007 года по настоящее время наблюдается тенденция к росту числа внутренних, так называемых «инсайдерских» ПАВ на информационно-телекоммуникационные сети. Если в 2007 г. было зарегистрировано всего 22 % мировых ИТС, подвергшихся внутренним ПАВ, то к 2010 г. доля их возросла уже до 58 %, причем большая часть из

них подверглась неизвестным для систем обнаружения воздействиям, доля которых приблизилась к отметке в 60 % от общего числа ПАВ.

Все вышеизложенное убедительно доказывает необходимость создания эффективных отечественных средств обнаружения и идентификации ПАВ. Однако основным препятствием на пути их создания является отсутствие адекватных моделей функционирования ИТС в условиях ПАВ, учитывающих не просто наличие или отсутствие факта воздействия на ИТС, а многоэтапность таких воздействий, поскольку любое типовое ПАВ само по себе может являться лишь одним из этапов более сложного и масштабного воздействия на ИТС.

Согласно разработанной в [3] классификации, любое ПАВ может быть разделено на четыре этапа реализации (рис. 1):

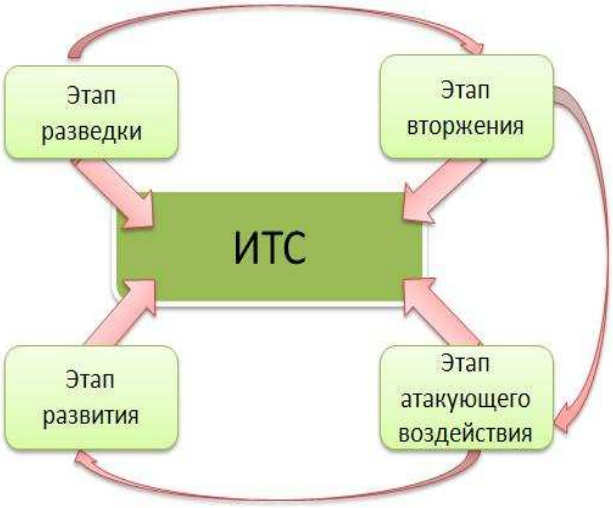


Рисунок 1. Этапы реализации ПАВ

- ***этап разведки***. На этом этапе злоумышленник осуществляет сбор данных о планируемом объекте ПАВ, на основе которых планируются ее дальнейшие этапы. Этап рекогносцировки включает в себя:

ПАВ

- изучение сетевого окружения;

- идентификация топологии ИТС;

- идентификация узлов ИТС;

- идентификация сервисов или сканирование портов;

- идентификация операционной системы;

- определение роли узла ИТС;

- определение уязвимостей узла ИТС.

- ***этап вторжения***. На данном этапе начинается попытка доступа к атакуемому узлу ИТС. При этом доступ может быть как непосредственный, т.е. проникновение на узел, так и опосредованный, например, при реализации программно-аппаратного воздействия типа "отказ в обслуживании". Реализация ПАВ в случае непосредственного доступа также может быть разделена на два этапа:

- проникновение;

- установление контроля.

- ***этап атакующего воздействия***. Данный этап направлен на достижение злоумышленником тех целей, ради которых предпринималось ПАВ. Примерами таких действий могут являться нарушение работоспособности аппаратных ресурсов ИТС, удаление или модификация данных системы и др.

Поскольку каждый из этапов может представлять собой самостоятельное воздействие, направленное на достижение лишь одной частной цели более сложного ПАВ, то и модель процесса функционирования ИТС в условиях ПАВ должна отражать поведение сети при реализации каждого из этих этапов. Поскольку целью разработки модели является отражение процесса функционирования ИТС на тех этапах ПАВ, когда оно еще может быть своевременно обнаружено, идентифицировано и, соответственно, предотвращено, то в качестве ограничения 4-й этап типового ПАВ не рассматривается, поскольку

направлен на дальнейшее развитие воздействия на ИТС, взаимодействующей с атакуемой.

В силу того, что состояние защищенности информационно-телекоммуникационной сети (ИТС) зависит от совокупности происходящих в этой сети событий, ее функционирование можно представить в виде нечеткой сети Петри [1,2].

Определим $S$ как множество состояний ИТС:

$$S = [S_1, S_2, S_3, S_4, S_5, S_6, S_7], \quad (1)$$

где $S_1$ – состояние нормального функционирования ИТС; $S_2$ – состояние проведения I этапа программно-аппаратного воздействия на ИТС; $S_3$ – состояние проведения II этапа программно-аппаратного воздействия на ИТС; $S_4$ – состояние проведения III этапа программно-аппаратного воздействия на ИТС; $S_5$ – состояние нарушения конфиденциальности ресурсов ИТС; $S_6$ – состояние нарушения целостности ресурсов ИТС; $S_7$ – состояние нарушения доступности ресурсов ИТС.

Пусть $K$ – множество событий в ИТС:

$$K = [K_1, \ldots, K_i], \qquad i \in N, \quad (2)$$

где $K_1$ – событие появления злоумышленника; $K_2$ – множество событий II этапа программно-аппаратного воздействия на ИТС; $K_3$ – событие срабатывания средств обнаружения и идентификации на I этапе программно-аппаратного воздействия на ИТС; $K_4$ – множество событий III этапа программно-аппаратного воздействия на ИТС; $K_5$ – множество событий, приводящих к нарушению конфиденциальности ресурсов ИТС; $K_6$ – множество событий, приводящих к нарушению целостности ресурсов ИТС; $K_7$ – множество событий, приводящих к нарушению доступности ресурсов ИТС; $K_8$ – множество событий восстановления ИТС после успешной реализации программно-аппаратного воздействия; $K_9$ – событие срабатывания средств обнаружения и идентификации на II этапе программно-аппаратного воздействия на ИТС; $K_{10}$ – событие срабатывания

средств обнаружения и идентификации на III этапе программно-аппаратного воздействия на ИТС;

Таким образом, множество событий в ИТС можно представить как объединение множеств указанных выше событий, т.е.:

$$K = K_1 \cup K_2 \cup K_3 \cup K_4 \cup K_5 \cup K_6 \cup K_7 \cup K_8 \cup K_9 \cup K_{10}. \quad (3)$$

Нечеткая сеть Петри может быть представлена в виде:

$$C_f = (N, f, \lambda, m_0), \quad (4)$$

где $N$ – структура НСП, $N=(P,T,I,O)$;

$f = (f_1, \dots, f_u)$ – вектор значений функции нечеткого срабатывания переходов, $f_j \in [0,1] \forall j \in \{1,2,\dots,u\}$; $\lambda = (\lambda_1, \dots, \lambda_u)$ – вектор значений порога срабатывания переходов, $\lambda_j \in [0,1] \forall j \in \{1,2,\dots,u\}$; $m_0$ – вектор начальной маркировки, $m_i^0 \in [0,1] \forall i \in \{1,2,\dots,n\}$.

Структура НСП $N=(P,T,I,O)$ аналогична структуре традиционных сетей Петри и может быть представлена следующими элементами:

$P = (p_1, \dots, p_n)$ – множество позиций НСП;

$T = (t_1, \dots, t_u)$ – множество переходов НСП, $u \in N$ ;

$I$ – входная функция переходов, $I: PxT \rightarrow \{0,1\}$;

O – выходная функция переходов.

Графически НСП представляет собой ориентированный двудольный мультиграф специального вида. На рисунке 2 представлена НСП для рассматриваемой ИТС. Здесь $S_1,\dots,S_7$ – множество состояний ИТС; $K_1,\dots,K_{10}$ – множество событий в ИТС; $t_1,\dots,t_{12}$ – соответствующие переходы ИТС из одного состояния $S_i$ в другое.

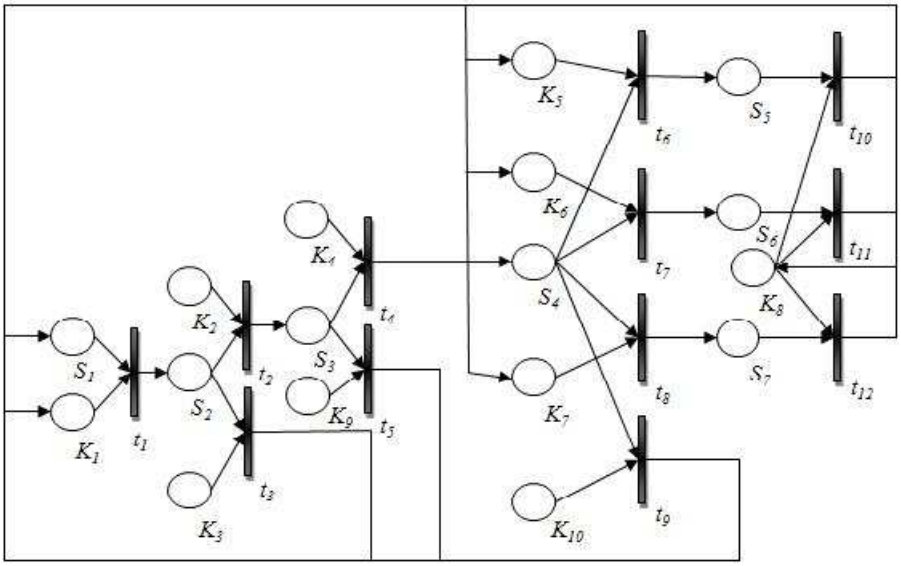


Рисунок 2. Структура НСП

Сформулируем базу правил нечеткого логического вывода:

Правило 1: **ЕСЛИ** «ИТС находится в состоянии нормального функционирования», **ТО** «при появлении злоумышленника ИТС переходит в состояние I этапа программно-аппаратного воздействия на ИТС».

Правило 2: **ЕСЛИ** «ИТС находится в состоянии I этапа программно-аппаратного воздействия», **ТО** «при срабатывании средств обнаружения и идентификации ПАВ ИТС переходит в состояние нормального функционирования».

Правило 3: **ЕСЛИ** «ИТС находится в состоянии I этапа программно-аппаратного воздействия», **ТО** «при появлении множества событий II этапа ПАВ ИТС переходит в состояние II этапа программно-аппаратного воздействия».

Правило 4: **ЕСЛИ** «ИТС находится в состоянии II этапа программно-аппаратного воздействия», **ТО** «при срабатывании средств обнаружения и идентификации ПАВ ИТС переходит в состояние нормального функционирования».

Правило 5: **ЕСЛИ** «ИТС находится в состоянии II этапа программно-аппаратного воздействия», **ТО** «при появлении множества

событий III этапа ПАВ ИТС переходит в состояние III этапа программно-аппаратного воздействия».

Правило 6: **ЕСЛИ** «ИТС находится в состоянии III этапа программно-аппаратного воздействия» **И** «злоумышленник нарушает конфиденциальность ресурсов ИТС», **ТО** «ИТС переходит в состояние нарушения конфиденциальности ресурсов».

Правило 7: **ЕСЛИ** «ИТС находится в состоянии III этапа программно-аппаратного воздействия» **И** «злоумышленник нарушает целостность ресурсов ИТС», **ТО** «ИТС переходит в состояние нарушения целостности ресурсов».

Правило 8: **ЕСЛИ** «ИТС находится в состоянии III этапа программно-аппаратного воздействия» **И** «злоумышленник нарушает доступность ресурсов ИТС», **ТО** «ИТС переходит в состояние нарушения доступности ресурсов».

Правило 9: **ЕСЛИ** «ИТС находится в состоянии III этапа программно-аппаратного воздействия», **ТО** «при срабатывании средств обнаружения и идентификации ПАВ ИТС переходит в состояние нормального функционирования».

Правило 10: **ЕСЛИ** «ИТС находится в состоянии нарушения конфиденциальности ресурсов» **И** «действует множество событий восстановления ИТС после программно-аппаратного воздействия», **ТО** «ИТС переходит в состояние нормального функционирования».

Правило 11: **ЕСЛИ** «ИТС находится в состоянии нарушения целостности ресурсов» **И** «действует множество событий восстановления ИТС после программно-аппаратного воздействия», **ТО** «ИТС переходит в состояние нормального функционирования».

Правило 12: **ЕСЛИ** «ИТС находится в состоянии нарушения доступности ресурсов» **И** «действует множество событий восстановления

ИТС после программно-аппаратного воздействия», **ТО** «ИТС переходит в состояние нормального функционирования».

Каждому предикату из вышеприведенных правил можно сопоставить определенную позицию НСП.

Сопоставим каждой позиции $P = \{p_1, \ldots, p_n\}$ элементы множества *S* и *K*.

$$P = \{S_1 K_1 S_2 K_2 K_3 S_3 K_9 K_4 S_4 K_{10} K_5 K_6 K_7 S_5 S_6 S_7 K_8\}$$

Определим вектор начальной маркировки:

$$m_0 = (m_1^0 m_2^0 m_3^0 m_4^0 m_5^0 m_6^0 m_7^0 m_8^0 m_9^0 m_{10}^0 m_{11}^0 m_{12}^0 m_{13}^0 m_{14}^0 m_{15}^0 m_{16}^0 m_{17}^0).$$

Здесь $m_i^0$ $(i = 1,3,6,9,14,15,16)$ – значение функций принадлежности наличия маркеров в позициях $S_1, S_2, S_3, S_4, S_5, S_6, S_7$, т.е. значения функций принадлежности нахождения ИТС в различных состояниях; $m_2^0$ – значение функции принадлежности наличия маркера в позиции $K_1$, т.е. фактически вероятность появления злоумышленника в ИТС; $m_1 k^T 0$ $(k = 5, 7, 10)$ – значение функций принадлежности наличия маркеров в позициях $K_2, K_9, K_{10}$, т.е. значение функций принадлежности возникновения событий срабатывания средств обнаружения и идентификации программно-аппаратных воздействий на ИТС на I, II и III этапах ПАВ; $m_1 j^T 0$ $(j = 11, 12, 13)$ – значение функций наличия маркеров в позициях $K_5, K_6, K_7$, т.е. значение функций принадлежности возникновения событий, приводящих к нарушению конфиденциальности, целостности и доступности ресурсов ИТС; $m_1 (u)^T 0$ $(u = 4,8)$ – значение функций принадлежности наличия маркеров в позициях $K_2, K_4$, т.е. значение функций принадлежности возникновения событий II и III этапа программно-аппаратного воздействия на ИТС; $m_{17}^0$ – значение функции принадлежности наличия маркера в позиции $K_8$, т.е. вероятность правильной реакции средств восстановления ресурсов ИТС после программно-аппаратного воздействия.

Для упрощения представленной модели примем: $m_1^0 = 1$, $m_{3,6,9,14,15,16}^0 = 0$, $m_{5,7,10,11,12,13}^0 = 1$, $f_{1-12} = 1$.

Рассмотрим последовательность переходов данной НСП. Динамика изменения маркировок НСП определяется следующими правилами:

1) *Правило определения текущей маркировки*. Любое состояние НСП определяется вектором $m$, компоненты которого интерпретируются как значения функции принадлежности нечеткого наличия одного маркера в соответствующих позициях НСП.
2) *Правило активности перехода*. Переход $t_k \in T$ является активным, если выполняется условие:

$$\min_{(i\in\{1,\dots,n\})\wedge(I(p_i,t_k)>0)} \{m_i\} \geq \lambda_k . \quad (5)$$

3) *Правило нечеткого срабатывания перехода*. Если переход $t_k \in T$ НСП является активным, то нечеткое срабатывание приводит к новой маркировке $m^y$, компоненты вектора которой определяются следующим образом:

$$m_i^y = 0, \qquad (\forall p_i \in P) \wedge (I(p_i,t_k) > 0), \quad (6)$$

$$m_j^y = \max\left\{m_j, \min_{(i\in\{1,\dots,n\})\wedge(I(p_i,t_k)>0)} [\{m_i, f_k\}\}, \qquad (\forall p_i \in P) \wedge (I(p_i,t_k) > 0)\right]$$

При начальной маркировке переход $t_1$ является активным при:

$$m_2^0 \geq \lambda_1, \quad (7)$$

т.е. в том случае, если вероятность появления злоумышленника в ИТС будет больше порога срабатывания перехода $t_1$. Допустим, что это условие выполняется, тогда нечеткое срабатывание перехода $t_1$ приведет к новой маркировке $m_1$. При этом $m_1^1 = m_2^1 = 0$, так как позиции $S_1$ и $K_1$ являются входными для перехода. Для позиции $S_2$ имеем $m_3^1 = \max\{[0, \min\{m_2^{0,1}\}\}$, т.е. $m_3^1 = m_2^0 \geq \lambda_1$. Все остальные позиции остаются без изменений. Для позиции $S_3$ имеем $m_6^2 = \max\{[0, \min\{m_4^{1,1}\}\}$, т.е. $m_6^2 = m_4^1 \geq \lambda_2$. Все остальные позиции остаются без изменений. Для позиции $S_4$ имеем $m_9^3 = \max\{[0, \min\{m_8^{2,1}\}\}$, т.е. $m_9^3 = m_8^2 \geq \lambda_4$. Все остальные позиции остаются без изменений. Поскольку

$m^3_{11,12,13} = 1$, то переходы $t_6, t_7, t_8$ будут активными при $m^3_6 \geq \lambda_6$, $m^3_6 \geq \lambda_7$, $m^3_6 \geq \lambda_8$. Переход $t_3$ будет активным при выполнении условия $\min\{m^1_3, m^1_5\} \geq \lambda_3$ или

$$\min\{m^0_2, m^0_5\} \geq \lambda_3 \quad (8)$$

Переход $t_5$ будет активным при выполнении условия $\min\{m^2_6, m^2_7\} \geq \lambda_5$ или

$$\min\{m^1_4, m^0_7\} \geq \lambda_5 \quad (9)$$

Переход $t_9$ будет активным при выполнении условия $\min\{m^3_9, m^3_{10}\} \geq \lambda_9$ или

$$\min\{m^2_8, m^0_{10}\} \geq \lambda_9 \quad (10)$$

Анализ выражений (7–10) показывает, что безопасная работа ИТС в условиях ПАВ может достигаться:

1) путем повышения коэффициента $\lambda_1$, что может быть достигнуто путем корректной настройки политики безопасности ИТС;

2) путем уменьшения коэффициентов $\lambda_3, \lambda_5, \lambda_9$, которые представляют собой порог чувствительности системы обнаружения и идентификации программно-аппаратных воздействий на различных этапах жизненного цикла ПАВ на ИТС.

3) путем увеличения коэффициентов $m^1_6, m^2_7, m^3_{10}$, которые характеризуют собой вероятность корректного обнаружения и идентификации программно-аппаратного воздействия на ИТС на различных этапах его жизненного цикла.

Однако стоит отметить, что уменьшение порога чувствительности системы обнаружения и идентификации программно-аппаратных воздействий на ИТС может привести к повышению числа ошибок 2 рода, когда нормальные процессы, происходящие в ИТС, будут идентифицированы системой обнаружения как программно-аппаратные воздействия, что в итоге приведет к снижению эффективности процесса обнаружения и идентификации ПАВ.

**Выводы:** разработанная модель процесса функционирования информационно-телекоммуникационной сети в условиях программно-аппаратных воздействий позволила определить параметры, влияющие на качество процесса обнаружения на каждом из трех основных этапов типового ПАВ, а также выявить зависимость этих параметров от значения вероятностей событий, происходящих в ИТС.

**Список литературы**

1. Васильев В.И., Кашаев Т.Р. Применение нечетких сетей Петри для анализа безопасности локальных вычислительных сетей // Вычислительная техника и новые информационные технологии: Межвузовский научный сборник. Вып. 6; УГАТУ. Уфа, 2007. С. 166–170.
2. Кашаев Т.Р. Моделирование состояния безопасности локальной вычислительной сети // Интеллектуальные системы обработки информации и управления: Материалы 2-й региональной зимней школы-семинара аспирантов и молодых ученых; УГАТУ. Уфа, 2008. С. 326–332.
3. Исупов А.Б., Юрков В.А., Королев И.Д., Скуратов В.Ю. Программно-аппаратные воздействия на АС ВН // Информационная безопасность – актуальная проблема современности: Материалы III научно-технической школы-семинары; Военная академия связи (филиал г. Краснодар). Краснодар, 2011. С. 58–61.
4. Исупов А.Б., Юрков В.А., Королев И.Д., Скуратов В.Ю. Роль и место процесса обнаружения и идентификации программно-аппаратных воздействий в обеспечении устойчивого функционирования автоматизированных систем военного назначения // Информационная безопасность – актуальная проблема современности: Материалы III научно-технической школы-семинары; Военная академия связи (филиал г. Краснодар). Краснодар, 2011. С. 6–11.Отчет CCIPS-2010 (Computer Crime and Intellectual Property Section) Министерства юстиции США, 2010. 72 с.