УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 150, кн. 4 Физико-математические науки *2008*

УДК 681.322

МАРКОВСКИЕ МОДЕЛИ СРЕДСТВ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Г.М. Тептин, К.В. Иванов

Аннотация

В работе выделяются характеристики образцов информационного оружия и строятся марковские модели функционирования коммутатора и межсетевого экрана. На основании построенных моделей делается оценочный расчёт характеристик рассматриваемых образцов и строится методика рассмотрения средств защиты с использованием теории марковских процессов.

Ключевые слова: марковские модели, коммутатор, межсетевой экран.

Введение

В рамках перехода от индустриального к информационному обществу, жизнедеятельность которого зависит от процессов сбора, хранения, передачи и обработки гражданской и военной информации, становятся чрезвычайно актуальными вопросы надёжной защиты информационной инфраструктуры государства, особенно его стратегической системы управления, а также оборонительных и ударных боевых систем от всех видов современного и перспективного информационного воздействия противника.

В настоящее время такой вид воздействия отечественные и зарубежные специалисты связывают с применением в противоборстве государств информационного оружия (ИО) [1–5].

Вероятностный подход широко используется при построении моделей функционирования средств защиты информации, так как только вероятностные модели, которые строятся на основе существующей автоматизированной системы (АС) и системы защиты, на данный момент способны дать количественную характеристику уровня защищенности системы. В работах [6–9] функционирование подсистемы защиты рассматривается отдельно от функционирования автоматизированной системы управления специального назначения или же затрагивается исключительно программное обеспечение. Вместе с тем существуют работы [10], описывающие использование теории очередей для анализа проектирования компьютерных сетей. В силу вышеизложенных причин весьма актуальным представляется построение вероятностных моделей функционирования защищенных АС в целом. Кроме того, модели не учитывают вероятность надежной работы системы, однако, надежность является не менее важным показателем среди других параметров безопасности. В большинстве моделей используются методы теории графов, а также содержатся предпосылки использования при построении моделей безопасности теории марковских процессов, что позволяет нам производить оценку защищённости и надежности как отдельных образцов ИО, так и систем защиты в комплексе, используя методы этих дисциплин.

Целью данной работы является разработка моделей ИО с использованием достижений теории графов, теории массового обслуживания (ТМО) и теории марковских процессов, а также построение методики рассмотрения образцов ИО на примере существующих средств защиты.

1. Информационное оружие – средство ведения информационной борьбы

Необходимые термины и определения, включая термины «информационное оружие», «информационное противоборство», вводятся в работе [12–14]. Следует отметить, что рассматриваемая проблема информационного противоборства значительно шире и глубже проблемы обеспечения информационной безопасности, так как последняя в основном рассматривается в существующей литературе ([4, 11] и др.) как совокупность методов и средств защиты информации от её несанкционированного использования и ликвидации злоумышленниками. Именно такой узкий подход, наряду с незавершённостью теории информационной безопасности общества, объясняет успехи компьютерной преступности в нарушении конфиденциальности, целостности и доступности данных военных и гражданских систем различного уровня.

Любой образец ИО, как и любое сложное средство вооружения, должен включать в себя две взаимодействующие компоненты:

– управляющая часть;

– исполнительная часть.

Назначением первой компоненты является управление исполнительной частью образца в процессе выполнения возложенных на него функций. Общая структура образца ИО представлена на рис. 1.

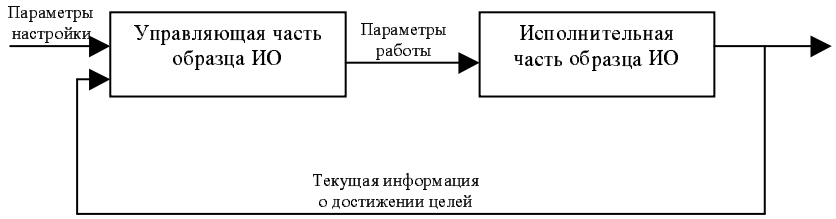

Рис. 1. Структура образца ИО

Образец ИО, функционирующий подобным образом, может быть рассмотрен в соответствии с моделью многодоступной вычислительной системы [15].

Рассмотрение модели ведётся при помощи методов теории массового обслуживания. Так как до сих пор мы рассматривали образец ИО в самом общем виде, необходима дальнейшая конкретизация, что влечёт за собой рассмотрение отдельных классов и образцов ИО и, как следствие, построение новых, более детализированных, моделей образцов ИО. Вместе с тем принципы [14], полагаемые в основу построения образцов ИО, налагают свои ограничения на совокупность характеристик образцов ИО.

Исходя из вышесказанного, для образцов ИО актуальными являются следующие группы характеристик:

- временные характеристики;
- ёмкостные характеристики;
- вероятностные характеристики.

Необходимо также принять во внимание, что ближайшим аналогом рассматриваемой нами в рамках данной работы автоматизированная система управления специального назначения (АСУ СН) является компьютерная сеть передачи данных на основе технологии Ethernet. Как показывает анализ литературы [16–19], методы ТМО в настоящее время находят широкое применение при проектировании, моделировании, а так же анализе производительности, надёжности и безопасности компьютерных сетей и АС в целом.

В рамках данной работы будем считать, что АСУ СН представляет собой совокупность узлов АСУ СН и межсетевых экранов, соединённых между собой посредством коммутаторов в соответствии со смешанной топологией и использующих для передачи данных технологию Ethernet и стек протоколов TCP/IP.

2. Марковская модель коммутатора

Пусть каждый порт представляет собой совокупность двух дисциплин обслуживания: дисциплина обслуживания принимаемых сообщений и дисциплина обслуживания приёма и передачи. Система массового обслуживания (СМО) может принимать следующие состояния:

S_0 – на входе нет пакетов;

S_1 – в СМО обрабатывается пакет;

S_2 – в СМО обрабатывается 1 пакет, при этом в буфере ожидания находится 1 пакет;

S_{L+1} – в СМО обрабатывается пакет, в очереди находится L пакетов;

S_{L+2} – буфер переполнен, система отбрасывает пакеты.

Таким образом, система представляет собой классическую марковскую цепь с интенсивностями переходов из состояния в состояние μ и λ соответственно.

Связь между вероятностями нахождения системы во всех его возможных состояниях $p_i(t)$ выражается системой дифференциальных уравнений Колмогорова.

Используем правила построения этих уравнений [20]: в левой части каждого уравнения записывается производная вероятности нахождения системы в рассматриваемом состоянии (вершине графа) $\dot{p}_i(t)$, а правая часть содержит столько членов, сколько ребер графа состояний связано с данной вершиной графа. Если ребро направлено из данной вершины, соответствующий член имеет знак «минус», если в вершину – знак «плюс». Каждый член равен произведению параметра (интенсивности) потока отказов (λ)или восстановлений (μ), связанного с данным ребром, на вероятность нахождения в той вершине графа, из которой исходит ребро $p_i(t)$.

Таким образом, необходимо решить систему дифференциальных уравнений:

$$\begin{aligned}
\dot{p}_0(t) &= -\lambda p_0(t) + \mu p_1(t),\\
\dot{p}_1(t) &= \lambda p_0(t) - (\lambda+\mu) p_1(t) + \mu p_2(t),\\
\dot{p}_2(t) &= \lambda p_1(t) - (\lambda+\mu) p_2(t) + \mu p_3(t),\\
\dot{p}_i(t) &= \lambda p_{i-1}(t) - (\lambda+\mu) p_i(t) + \mu p_{i+1}(t),\\
\dot{p}_{L+2}(t) &= \lambda p_{L+1}(t) - \mu p_{L+2}(t).
\end{aligned}$$

Решение данной системы позволяет получить функциональную зависимость вероятностных характеристик системы от времени.

Из приведённых выше выкладок следует, что исследуемые характеристики весьма существенно зависят от интенсивности входного потока и интенсивности обработки кадров. Если интенсивность обработки кадров напрямую зависит от технологий, применяемых при синтезе коммутаторов, то интенсивность входного потока может меняться в широких пределах. Обсудим состав входного потока.

Для передачи данных в сетях Ethernet в настоящее время используются следующие стандарты:

• Ethernet (10 Мбит/с). Максимальная пропускная способность сегмента Ethernet составляет 14880 кадр/с для кадров минимальной длины и 813 кадр/с для кадров максимальной длины. Соответственно, реальная максимальная производительность такой сети колеблется от 5.48 Мбит/с для кадров минимальной длины до 9.76 Мбит/с для кадров максимальной длины [21].

• Fast Ethernet (100 Мбит/с). Механизм CSMA/CD в сети Fast Ethernet работает так же, как и в сети Ethernet 10 Мбит/с, и пакеты имеют аналогичный размер, но их скорость распространения через среду передачи в десять раз выше за счёт изменений в средствах физического уровня [21]. Исходя из этих предпосылок будем считать, что максимальная пропускная способность сегмента Fast Ethernet составляет 148800 кадр/с для кадров минимальной длины и 8130 кадр/с для кадров максимальной длины, а максимальная производительность такой сети колеблется соответственно от 54.8 до 97.5 Мбит/с, что составляет 7986 пакетов/с.

• Gigabit Ethernet (1000 Мбит/с). Реализация данного стандарта в настоящее время получает всё большее распространение, однако на практике он используется чрезвычайно редко, поэтому мы исключаем его из рассмотрения.

Таким образом, в расчётах интенсивность входного потока колеблется в пределах от 0.000813 до 0.1488 кадр/мкс.

Вместе с тем необходимо учесть, что на обработку каждого кадра независимо от его длины коммутатор тратит примерно равное время, и, соответственно, наиболее тяжёлый режим работы будет создаваться при обработке потока кадров минимальной длины. Рассчитаем значения вероятностей в соответствии с исходными данными, приведёнными в работе [22] и оценим возможность реализации атаки отказа в обслуживании.

Для приёмного тракта порта коммутатора $\lambda = 0.1488$ кадр/мкс, $\mu = 0/1859$ кадр/мкс минимально используемый размер буферной памяти $L = 4$ кадра. Результаты решения системы дифференциальных уравнений приведены на рис. 2.

Таким образом, можно считать, что на этапе приёма кадров коммутатором вероятность потери кадров (успешной реализации атаки отказа в обслуживании) p6 не превышает 0.08, и при дальнейших расчётах ею можно пренебречь.

Поток кадров, передаваемых на i-й порт, в общем случае имеет интенсивность

$$\lambda_{i\text{пер}} = (1 - P_{\text{пот1}}) \sum_{j=i}^{n-1} \lambda P_{ij} \simeq \sum_{j=i}^{n-1} \lambda P_{ij},$$

где $i \neq j$, P_{ij} – вероятность того, что кадры, поступившие с j-го порта, имеют адрес назначения на i-м порту, – количество портов в коммутаторе, а $P_{\text{пот1}}$ – вероятность потери кадров в приёмном тракте. При расчёте вероятностей состояний передающего тракта коммутатора в рамках данной работы примем следующие допущения.

Результаты решения системы дифференциальных уравнений для равновероятной передачи пакетов во все порты коммутатора ($n = 8$) приведены на рис. 3. Результаты решения системы дифференциальных уравнений для случая, когда интенсивность входящего потока кадров превышает интенсивность передачи кадров (атака отказа в обслуживании) приведены на рис. 4 (размер буферной памяти $L = 4$ кадра) и на рис. 5 (размер буферной памяти $L = 22$ кадра).

Как видно из соответствующих графиков, наиболее вероятна успешная реализация атаки отказа в обслуживании, направленная на передающий тракт портов

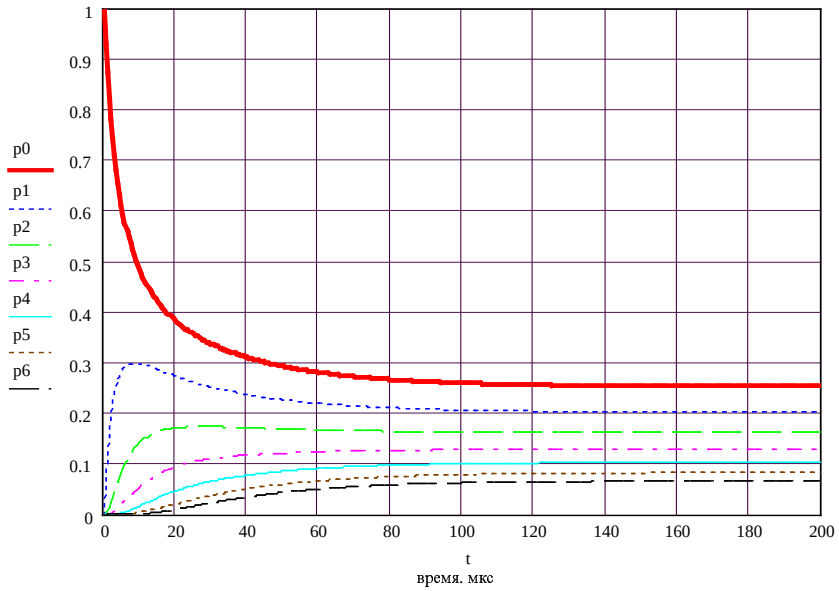

Рис. 2. Вероятности состояний тракта приёмного тракта коммутатора с длиной буфера 4 кадра

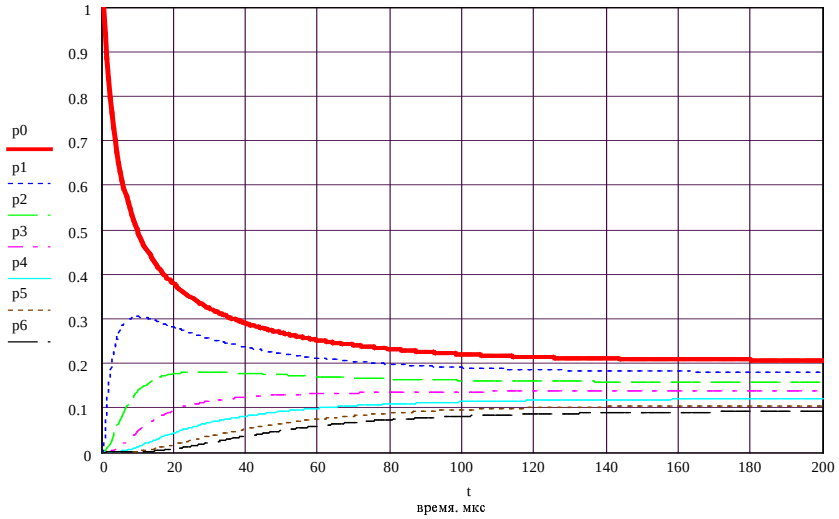

Рис. 3. Вероятности состояний тракта передающего тракта коммутатора с длиной буфера 4 кадра. Равновероятное распределение кадров

коммутатора. Однако время, необходимое для реализации такой атаки, может быть существенно увеличено (в рассмотренном примере со 100 до 400 мкс), а сама вероятность успешной реализации атаки снижена за счёт увеличения объёма буферной памяти передающего тракта порта коммутатора. Данные выводы подтверждаются экспериментальными данными, полученными в работе [22].

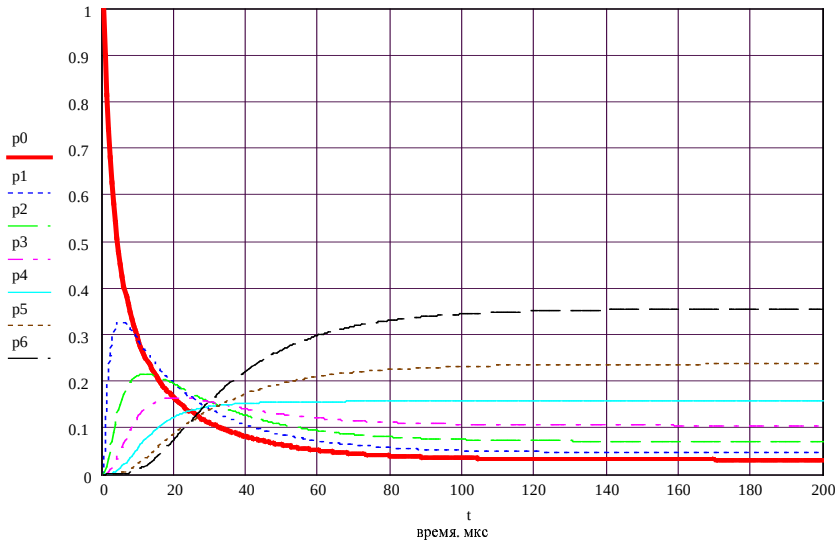

Рис. 4. Вероятности состояний тракта передающего тракта коммутатора с длиной буфера 4 кадра. Атака отказа в обслуживании

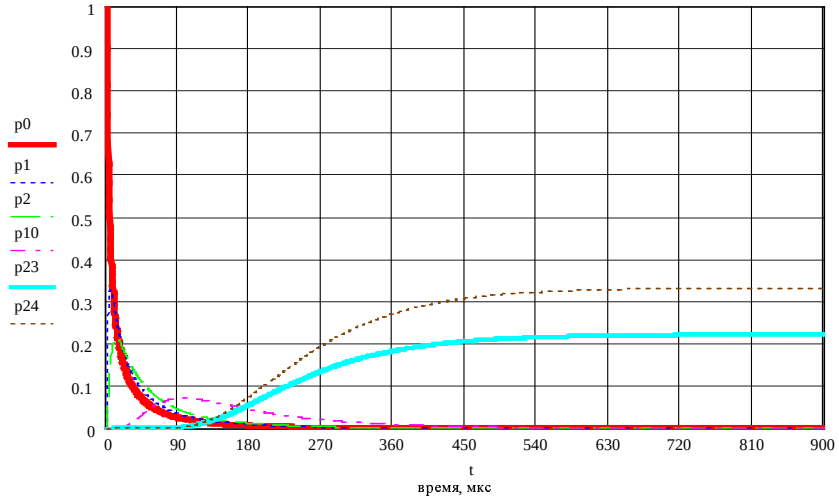

Рис. 5. Вероятности состояний тракта передающего тракта коммутатора с длиной буфера 22 кадра. Атака отказа в обслуживании

3. Марковская модель межсетевого экрана

Межсетевой экран (МЭ) – это программный или аппаратно-программный комплекс, реализующий функции фильтрации сетевого трафика (информационных потоков) между двумя и более автоматизированными системами по некоторому набору правил (базе правил или БП), определяемых политикой безопасности (ПБ) [23]. Необходимо отметить, что в современные МЭ зачастую включают дополнительные средства защиты. Это обусловлено тем, что МЭ устанавливается на границе нескольких АС и расширение его функционала является весьма удобным. Результаты рассмотрения существующих типов МЭ приводятся в работе [23].

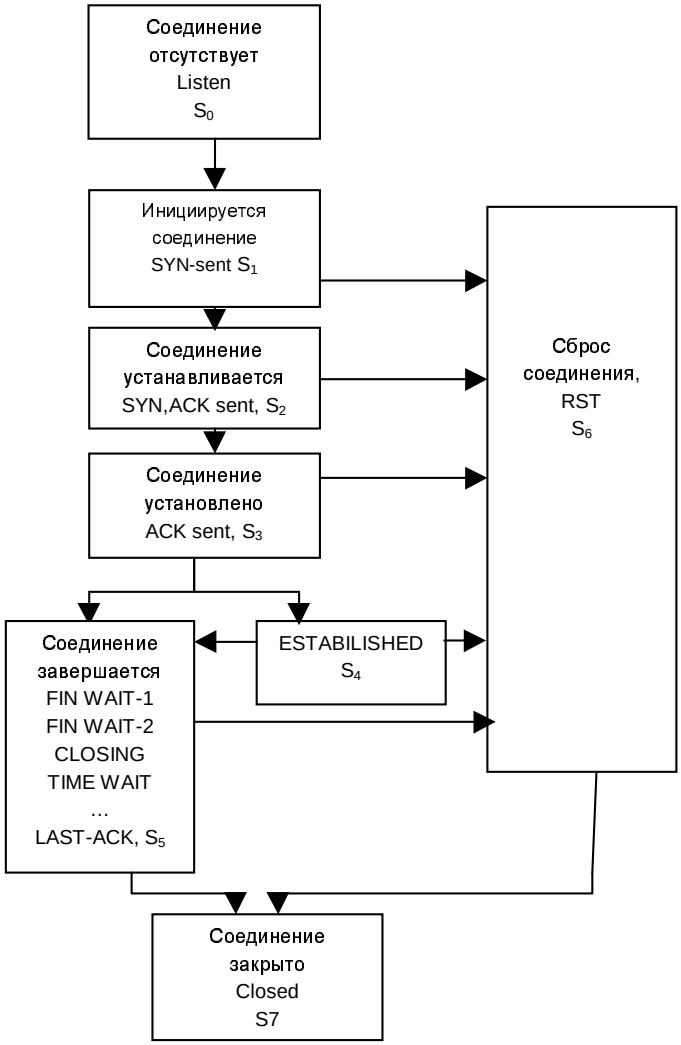

Рис. 6. Схема переходов между состояниями TCP-соединения

В рамках данной работы рассмотрим модель межсетевого экрана-инспектора состояний. Инспекторы состояний позволяют контролировать не отдельные пакеты трафика, а потоки трафика от источника к приёмнику. Далее такие потоки мы будем называть соединениями. Каждое соединение контролируется в зависимости от используемых протоколов на основе таблиц состояний, что позволяет отсеивать некорректно работающие соединения. Дополнительно контролируется время устаревания соединения: если между обработкой пакетов, принадлежащих одному потоку, проходит время, большее, чем установлено в МЭ как время устаревания соединения, такое соединение прекращается. Рассмотрим работу инспекторов состояний на примере протокола TCP.

В работе [24] приводится схема переходов между состояниями TCP-соединения. Однако для МЭ не имеет значения, с какой стороны инициируется соединение. Схема переходов между состояниями TCP-соединения для межсетевого экрана изображена на рис. 6. Следовательно, у нас имеется граф переходов между состояниями МЭ. Состояние «сброс соединения» возникает в случае аномального поведения хостов-участников соединения.

Аналогично тому, как это было сделано при построении модели коммутатора, построим систему дифференциальных уравнений:

$$\begin{aligned}
\dot{p}_0(t) &= -\lambda_{01} p_0(t),\\
\dot{p}_1(t) &= \lambda_{01} p_0(t) - (\lambda_{16} + \lambda_{12}) p_1(t),\\
\dot{p}_2(t) &= \lambda_{12} p_1(t) - (\lambda_{26} + \lambda_{23}) p_2(t),\\
\dot{p}_3(t) &= \lambda_{23} p_2(t) - (\lambda_{36} + \lambda_{34} + \lambda_{35}) p_3(t),\\
\dot{p}_4(t) &= \lambda_{34} p_3(t) - (\lambda_{46} + \lambda_{45}) p_2(t),\\
\dot{p}_5(t) &= \lambda_{35} p_3(t) + \lambda_{45} p_4(t) - \lambda_{57} p_5(t),\\
\dot{p}_6(t) &= \lambda_{16} p_1(t) + \lambda_{26} p_2(t) + \lambda_{36} p_3(t) + \lambda_{46} p_4(t) - \lambda_{67} p_6(t),\\
\dot{p}_7(t) &= \lambda_{57} p_5(t) + \lambda_{67} p_6(t).
\end{aligned}$$

Начальные условия этой системы дифференциальных уравнений имеют вид

$$p_0(0) = 1, \quad p_i(0) = 0, \quad i = 1, \ldots, 7.$$

Решения задачи Коши должны удовлетворять условию нормировки

$$\sum_{i=0}^{7} p_i(t) = 1, \quad t \in [0, \infty),$$

которое означает, что в любой момент времени процесс функционирования инспектора состояний должен находиться в одном из состояний $s_i,\ i = 1, \ldots, 7$.

Обсудим интенсивности переходов. В силу того, что на обработку каждого IP-пакета независимо от его длины МЭ тратит примерно равное время, наиболее тяжёлый режим работы будет создаваться при обработке потока IP-пакетов минимальной длины.

Минимальный размер поля данных кадра Ethernet – 64 байт. Максимальный размер IP-заголовка – 60 байт. Таким образом, на область данных остаётся 4 байта и в первом приближении можно считать, что количество IP-пакетов соответствует количеству кадров канального уровня. Соответственно, для модели справедливы рассуждения, проведённые для коммутаторов, и интенсивность потока пакетов (интенсивность соединения) колеблется в пределах от 0.000813 до 0.1488 кадр/мкс.

Пусть во время установления соединения перехват соединения нарушителем невозможен. Тогда интенсивности переходов между состояниями S0, S1, S2, S3 соответствуют интенсивностzm соединения.

Сброс соединений производится в соответствии со спецификацией [24], а также зависит от настроек, выставленных на МЭ. В рамках данной модели будем считать, что сбросом соединений в соответствии со спецификацией можно пренебречь. Так как время жизни пакета не превышает нескольких десятков секунд [24], в рамках данной работы будем считать его равным 50 с. Соответственно, настроим МЭ на разрыв соединения, если в течение 50 с не поступило ни одного пакета, принадлежащего этому соединению, то есть

$$\lambda_{16} = \lambda_{26} = \lambda_{36} = \lambda_{156} = 0.02 \cdot 10^{-6} \text{ пакетов/мкс}.$$

Однако необходимо учитывать, что интенсивность перехода имеет приведённое выше значение только в том случае, если на вход инспектора состояний не поступают пакеты с некорректным расположением флагов (например, не проводится

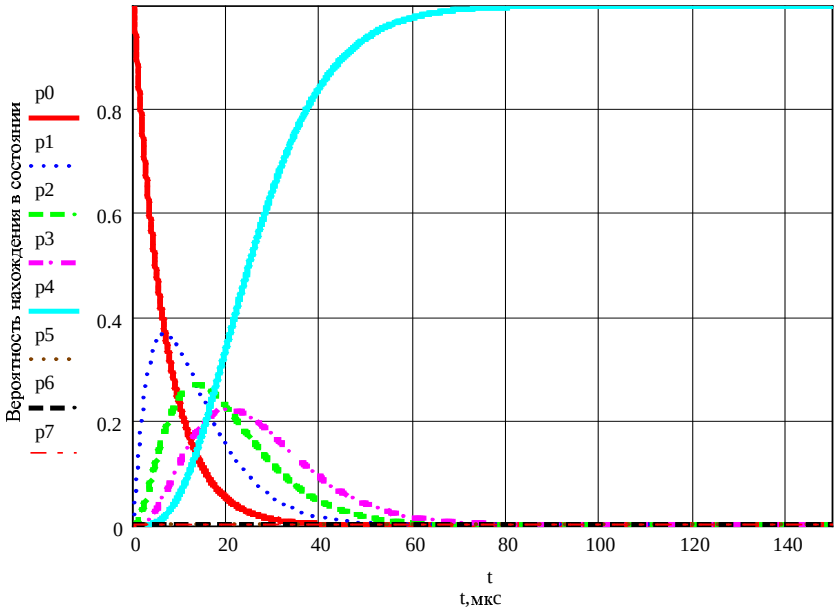

Рис. 7. Вероятности состояний инспектора TCP-состояний

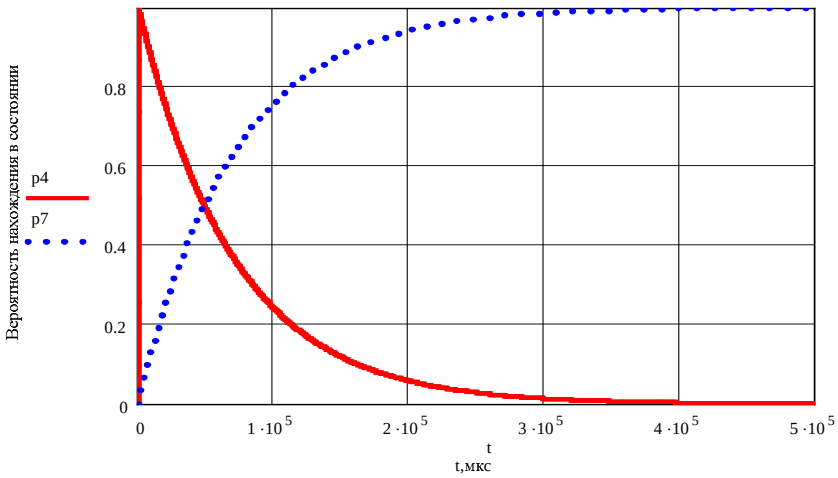

Рис. 8. Вероятности состояний инспектора TCP-состояний

атака, известная как «рождественская ёлка»). В противном случае интенсивность отбрасывания пакетов на МЭ будет выше.

Интенсивность переходов к завершению соединения зависит от времени, в течение которого используется сессия. Будем считать, что интенсивность перехода из состояния, соответствующего передаче данных, $\lambda_{45} = 0.000014$ пакетов/мкс, а сброс соединения сразу после его создания $\lambda_{35} = 0.003 \cdot 10^{-7}$ пакетов/мкс.

Интенсивность закрытия соединения определяется реализацией технологии межсетевого экранирования. В рамках настоящего расчёта примем её равной максимальной интенсивности потока пакетов: $\lambda_{67} = \lambda_{57} = \lambda$.

Результаты решения соответствующей системы уравнений для рассмотренных оценочных значений λ_{ij} приведены на рис. 7, 8. Построенная модель TCP-

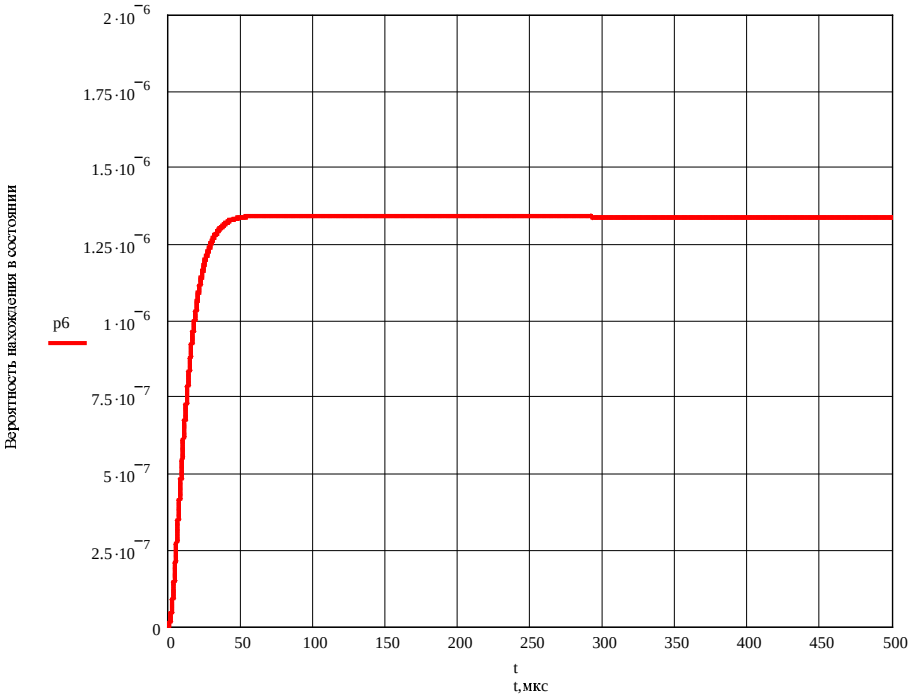

Рис. 9. Зависимость вероятности отбрасывания некорректных пакетов от времени

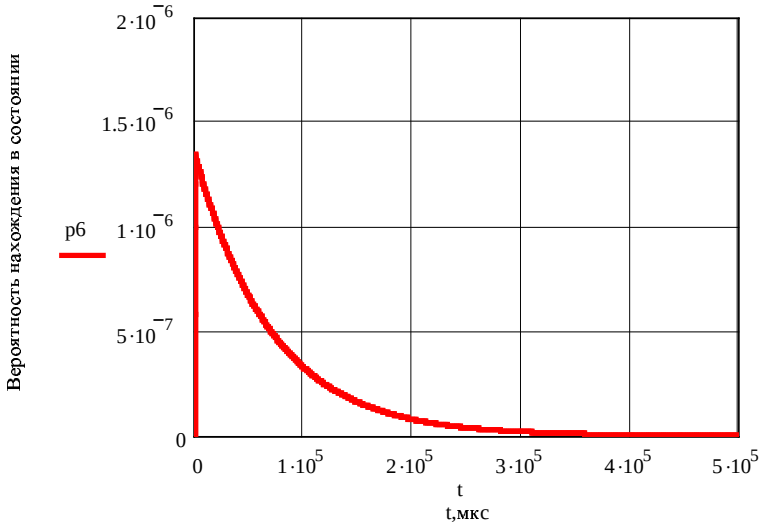

Рис. 10. Зависимость вероятности отбрасывания некорректных пакетов от времени

соединения позволяет оценить время, необходимое для организации такого соединения. Приведённый выше оценочный расчёт позволяет продемонстрировать форму графиков вероятностных характеристик состояний межсетевого экрана. Необходимо также отметить, что вероятность отбрасывания некорректных пакетов трафика при нормальной работе сети не превышает значения $1.4 \cdot 10^{-6}$ (рис. 9), а по завершении соединения составляет величину порядка 10^{-9} (рис. 10). Это го-

ворит о том, что при работе инспектора состояний доля отсекаемого им трафика весьма мала.

Точки максимумов вероятностей $p_1(t),\ p_2(t),\ p_3(t)$ – это наиболее вероятные моменты времени, когда инспектор состояний находится в соответствующих состояниях. Таким образом, запрос нового соединения наиболее вероятен через каждые 6 мкс, создание нового соединения начнётся через 13 мкс, а установится соединение через 20 мкс начиная с момента начала наблюдения. Как показывают приведённые выше графики, вероятности всех возможных состояний по мере передачи пакетов последовательно проходят свой максимум, после чего стремятся к стационарному значению, которое равно нулю для $S_0,\ S_1,\ S_2$. Для всех остальных вероятностей, кроме вероятности закрытия соединения, стационарное значение весьма близко к 0. Вероятность закрытия соединения стремится к единице.

Заключение

Из результатов анализа функционирования рассмотренных средств защиты следует вывод, что методика рассмотрения включает в себя следующие этапы:

- проводится анализ функционирования данного средства защиты или системы в целом и построение спецификации;
- для расчёта ёмкостных и временных характеристик строится многофазная система массового обслуживания, необходимые характеристики получаются суммированием соответствующих характеристик для каждой фазы;
- для расчёта вероятностных характеристик производится формализация всех возможных состояний соответствующей системы;
- выделяются безопасные и небезопасные состояния;
- определяются интенсивности переходов средства защиты из одного состояния в другое;
- строится граф переходов из состояния в состояние;
- в соответствии с графом строится система дифференциальных уравнений Колмогорова;
- по результатам решения системы уравнений Колмогорова определяются вероятностные характеристики состояний системы как функции времени.

На основании оценочных расчётов и экспериментальных данных, полученных для коммутатора, сделан вывод, что атака отказа в обслуживании реализуется с более высокой вероятностью на передающий тракт порта коммутатора. Для снижения вероятности успешной атаки, а также для замедления процесса атаки рекомендуется увеличивать размеры буферной памяти передающего тракта. Построенная модель инспектора состояний TCP-соединения позволяет оценить время, необходимое для организации такого соединения. Приведённый оценочный расчёт позволяет продемонстрировать форму графиков вероятностных характеристик состояний межсетевого экрана.

Разработанные модели межсетевых экранов планируется использовать в информационной системе, связывающей кластер параллельных вычислений и систему сбора данных сети приемников ГЛОНАСС-GPS.

Результаты статьи получены частично в рамках реализации Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России».

Summary

G.M. Teptin, K.V. Ivanov. Markov models of Defense Means for Automated Special-Purpose Systems.

The paper specifies characteristics of information weapon samples. Markov models of switch and firewall functioning are built. On the basis of these models the evaluated calculations of the sample characteristics are carried out and the method of the defense means viewing is formed using Markov process theory.

Key words: Markov models, switches, firewalls, DOS-attacks.

Литература

1. *Слипченко В.И.* Войны шестого поколения. Оружие и военное искусство будущего. – М.: Вече, 2002. – 384 с.
2. *Гриняев С.Н.* Интеллектуальное противодействие информационному оружию. – М.: Синтег, 1999. – 232 с.
3. *Прокофьев В.Д.* Тайное оружие информационной войны. Серия: Информатизация Россия на пороге XXI века. – М.: Синтег, 1999. – 152 с.
4. *Киселёв В.Д., Есиков О.В., Кислицын А.С.* Защита информации в системах её передачи и обработки / Под ред. Е.М. Сухарёва. – М.: Солид, 2000. – 200 с.
5. *Отюцкий Г.П.* К вопросу о сущности военно-технической революции // Военная мысль. – 1998. – № 2.
6. *Голубев В.О.* Розслідування комп'ютерних злочинів. - Запоріжжя: Гуманітарний університет «ЗІМТУ», 2003. – 296 с.
7. *Шриниваc В.* Качество обслуживания в сетях IP. / Пер. с англ – М.: Изд. дом «Вильямс», 2003. – 368 с.
8. *Ларионов А.М. и др.* Вычислительные комплексы, системы и сети. – Л.: Энергоатомиздат, 1987. – 288 с.
9. *Томашевський О.В.* Визначення надійності технічних засобів захисту інформації // Інформаційні технології та захист інформації: Зб. наук. праць. – 1999. – № 1. – С. 97-103.
10. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с.
11. *Мельников В.А.* Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. 368 с.
12. *Расторгуев С.П.* Информационная война. Проблемы и модели. Экзистенциальная математика – М.: Гелиос АРВ, – 2006. 240 с.
13. *Гриняев С.Н.* Поле битвы - киберпространство: теория, приёмы, средства, методы и системы ведения информационной войны – Минск: Харвест, 2004. – 448 с.
14. *Иванов К.В.* Системотехника средств поражения и защиты автоматизированных систем управления специального назначения. // Наука. Промышленность. Оборона. Труды VII Всерос. науч.-техн. конф. – Новосибирск: НГТУ, 2006. – С. 172–176.
15. *Авен О.П., Гурин Н.Н., Коган Я.А.* Оценка качества и оптимизация вычислительных систем. – М.: Наука, 1982. – 464 с.
16. Современные технологии коммутации (уровни коммутации). – URL: http://itelltd.kiev.ua/?page=articles&aid=35.
17. *Макаренко А.В.* Модель динамики коммутатора Gigabit Ethernet // Журн. радиоэлектроники. – 2001. – № 11. – URL: http://jre.cplire.ru/jre/nov01/2/text.html.

18. *Тихоненко О.М.* Модели массового обслуживания в информационных системах. – Минск: УП «Технопринт», 2003. – 327 с.

19. *Щеглов А., Щеглов К.* Компьютерная безопасность. Часть 7. Оценка влияния добавочных средств защиты от несанкционированного доступа на загрузку вычислительного ресурса защищаемого объекта. – 2005. – URL: http://daily.sec.ru/dailypblshow.cfm?rid=45&pid=12453.

20. *Пискунов Н.С.* Дифференциальное и и интегральное исчисления для ВТУЗов. – М. Физматгиз, 1961. – 748 с.

21. *Олифер В.Г., Олифер Н.А.* Компьютерные сети: принципы, технологии, протоколы. – М.: Питер, 2006. – 957 с.

22. *Иванов К.В.* Расчёт размеров буферной памяти и времени задержки кадров в коммутаторе OptiSwitch // Вестн. КГТУ. – 2007. – № 4. – С. 57–60.

23. *Лебедь С.В.* Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: Изд-во МГТУ им. Баумана, 2002. – 304 с.

24. Протокол управления передачей. Программная спецификация протокола DARPA INTERNET // Разумные сети от компании BiLiM Systems. – URL: http://www.protocols.ru/files/RFC/rfc793.pdf.

Поступила в редакцию
14.04.08

Тептин Герман Михайлович – доктор физико-математических наук, профессор, заведующий кафедрой радиоастрономии Казанского государственного университета.

E-mail: *Guerman.Teptin@ksu.ru*

Иванов Константин Васильевич – ассистент кафедры радиоастрономии Казанского государственного университета.

E-mail: *kivanov@icl.kazan.ru*