DOI: 10.36535/0236-1914-2022-01-6

УДК 681.3.06

ИМИТАЦИОННОЕ ДИСКРЕТНО-СОБЫТИЙНОЕ МОДЕЛИРОВАНИЕ СТОХАСТИЧЕСКИХ ПРОЦЕССОВ СЕТЕВЫХ АТАК НА УЗЛЫ СВЯЗИ ТРАНСПОРТНОЙ СИСТЕМЫ И АКТИВНОГО ПРОТИВОДЕЙСТВИЯ ИМ

Доктор техн. наук, профессор **Лозовецкий В.В.**
(МГТУ им. Н.Э. Баумана)

Кандидат техн. наук, доцент **Лебедев В.В.,**
кандидат техн. наук, доцент **Шукенбаев А.Б.**
(Российский технологический университет. МИРЭА)

Начальник научно-исследовательской лаборатории **Сергущенко А. В**.
(ФГКУ "12 ЦНИИ" Минобороны России)

Кандидат техн. наук **Архипенко А.В.**
(Сочинский международный инновационный университет)

DISCRETE-EVENT SIMULATION OF STOCHASTIC PROCESSES OF NETWORK ATTACKS ON COMMUNICATION NODES OF THE TRANSPORT SYSTEM AND ACTIVE COUNTERACTION TO THEM

Doctor (Tech.), Professor **Lozovetsky V.V.**
(Moscow State Technical University N.E.Bauman)

Ph.D. (Tech.), Associate Professor **Lebedev V.V.,**
Ph.D. (Tech.), Associate Professor **Shukenbaev A.B.**
(Russian Technological University. MIREA)

Head of the Research Laboratory **Sergushchenko A.V.**
(FGKU "12 Central Research Institute" of the Ministry of Defense of Russia)

Ph.D. (Tech.) **Archipenko A.V.**
(Sochi International Innovative University)

Узлы связи транспортной системы, показатели надёжности защиты, имитационная модель сценария атаки, стохастическая система, локальная вычислительная сеть, вредоносный контент, вероятностные параметры, система защиты, система массового обслуживания, модель восстановления, каналы обслуживания.

Communication nodes of the transport system, protection reliability indicators, simulation model of attack scenario, stochastic system, local area network, malicious content, probabilistic parameters, protection system, queuing system, recovery model, service channels.

Рассматриваются алгоритмы имитационного моделирования дискретных стохастических процессов развития сетевых атак и противодействия им, причём автоматизированная информационная система, имеющая в своём составе автоматизированную подсистему защиты, рассматривается как система с отказами-восстановлениями. Подзадача динамического баланса потока отказов и восстановлений в данной работе рассматривается в рамках математической схемы системы массового обслуживания. Показана возможность моделирования статистических параметров динамических свойств системы. Показана возможность применения алгоритма к исследованию характеристик надёжности подсистем автоматизированной динамической защиты автоматизированных информационных систем, в том числе информационные системы объектов критической информационной инфраструктуры.

The article discusses algorithms for simulation of discrete stochastic processes of development of network attacks and counteraction to them, moreover, an automated information system, which includes an automated protection subsystem, is considered as a system with failures-recoveries. The sub-problem of the dynamic balance of the flow of failures and restorations in this work is considered within the framework of the mathematical scheme of the mass service system. The possibility of modeling the statistical parameters of the dynamic properties of the system is shown. The possibility of applying the algorithm to the study of the reliability characteristics of automated dynamic protection subsystems of automated information systems, including information systems of critical information infrastructure objects, is shown.

1. Алгоритмы имитационного моделирования сценариев развития сетевых атак и процессов противодействия им

Исследование динамических характеристик процессов противодействия сетевым атакам необходимо на этапе проектирования систем защиты автоматизированных информационных систем. Главной целью при этом может стать определение необходимых темпов проведения операций по своевременному выявлению и нейтрализации таких угроз со стороны автоматизированных систем защиты информации в целях минимизации ущерба.

Динамика процесса реагирования на события, связанные с выявлением отказов компонентов автоматизированных информационных систем, непосредственно связана с динамикой самого процесса атаки.

Отказ интерпретируем, в соответствии с теорией надёжности [1-3], как некоторое отклонение в характеристиках функционирования системы или её компонентов, которое выходит за установленные нормативные пределы и рассматривается как нарушение работоспособности.

Процесс атаки, как правило, можно представить как некоторый стохастический процесс в виде цепочки событий, возникающих в системе в последовательные, но случайные моменты времени. Сценарий развития во времени процесса противодействия атаке связан, таким образом, со случайными моментами времени, в которые происходит обнаружение некоторых признаков вредоносных воздействий атаки на узлы связи, в частности, транспортной системы. В течение некоторого, в общем случае, случайного по длительности периода, после этих моментов времени, происходит анализ характера воздействия, принимается решение о способах нивелирования угрозы и производится операция по восстановлению работоспособности системы. Таким образом, автоматизированную информационную систему, имеющую активную систему защиты, в рамках предлагаемого подхода можно моделировать как систему с динамическим случайным по времени процессом потока отказов и восстановлений работоспособности.

Имеет место дискретно-событийный характер изменений в рассматриваемом случайном процессе: в случайные дискретные моменты времени в системе дискретно изменяется количество отказавших и восстановленных узлов. Динамику процессов атаки и противодействия ей предлагается исследовать методами имитационного моделирования.

В условиях постоянной угрозы компьютерных инцидентов решение задач безопасного управления автоматизированными информационными системами объектов критической информационной инфраструктуры занимает пристальное внимание исследователей [4-6]. В этой связи также заслуживает внимания исследование динамических характеристик развития атак на распределённые полевые и прочие информационные сетевые структуры управления. Противодействие атакам на информационные активы и нивелирование угроз должно быть своевременным. Моделирование позволяет установить прогнозные, необходимые при проектировании, оптимальные динамические параметры автоматизированных систем активной защиты.

Ниже рассмотрены подходы к моделированию процессов сетевых атак и процессов противодействия им со стороны автоматизированных систем защиты. Предлагаемые модели позволяют строить шкалы случайных моментов времени, в которые дискретно изменяется состояние системы. Таким образом, сценарий изменения состояний системы моделируется как дискретная цепочка событий, представляющих множество возникающих в системе отказов и следующих за ними операциями устранения отказов – восстановлением работоспособности. Так строится траектория случайного дискретного процесса изменения состояния системы. Исследование траекторий случайных процессов даёт возможность оценивать их динамические характеристики и вычислять статистические параметры надёжности систем защиты.

2. Имитационная дискретно-событийная модель сетевой атаки

Сложность проблемы математического моделирования связана со стохастическим характером процессов и разнообразием структурных параметров локальных вычислительных сетей (ЛВС) рассматриваемых объектов.

Алгоритм имитационной модели дискретного случайного процесса сетевой атаки рассмотрен в работе [7]. Для целостного рассмотрения обсуждаемой задачи приведём кратко основные параметры модели сетевой атаки. В математической модели рассматривается сценарий развития случайного дискретного процесса атаки на ЛВС.

Происходит распространение вредоносного контента (ВК), источником которого выступает трафик, содержащий в отдельных фрагментах ВК. Трафик может быть внешним по отношению к ЛВС или исходить из некоторых узлов. Рассматривается ординарный разреженный случайный процесс распространения ВК, который характеризуется случайными интервалами времени между появлениями ВК на входе в узлы сети.

Выбор направления трафика на узлы сети имеет случайный характер. Также вероятностный характер имеет и поступление ВК на выбранный случайный узел и факт успешного завершения атаки на узел в этом случае.

ВК в аспекте рассматриваемых проблем может представлять угрозу компрометации информационных ресурсов системы посредством перехвата и несанкционированного доступа с целью кражи, раскрытия или искажения информации, нарушения работоспособности объекта управления, установления удалённого управления элементами полевой структуры и т.п.

Интенсивность атаки на сеть в модели предлагается связать с интенсивностью дискретного потока сообщений на входной сетевой узел с учётом последующего включения в этот процесс узлов, заражённых ВК. Структура взаимодействия узлов сети между собой представлена орграфом (рис. 1).

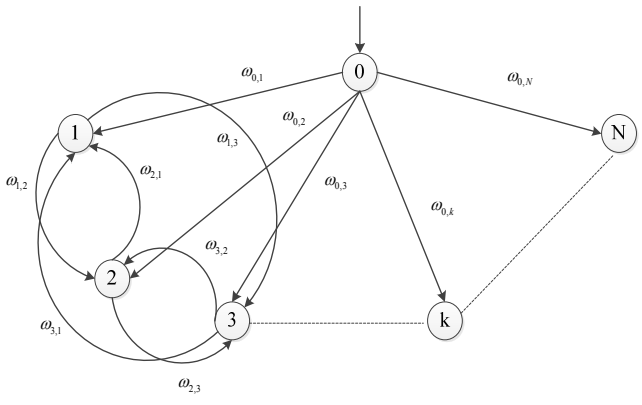

Рис. 1.Схема графа связи между узлами ЛВС

Темп информационного взаимодействия узлов сети характеризуется матрицей частости:

$$\Omega = \begin{bmatrix} \omega_{0,0} & \omega_{0,1} & \dots & \omega_{0,k} & \dots & \omega_{0,N} \\ \omega_{1,0} & \omega_{1,1} & \dots & \omega_{1,k} & \dots & \omega_{1,N} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \omega_{k,0} & \omega_{k,1} & \dots & \omega_{k,k} & \dots & \omega_{k,N} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \omega_{N,0} & \omega_{N,1} & \dots & \omega_{N,k} & \dots & \omega_{N,N} \end{bmatrix}$$

Частота $\omega_{i,j}$ входящих обращений из i - го узла в j - й узел определяется как отношение трафика между узлами i и j на сумму трафика в j - м столбце, которая равна общему трафику, входящему в j - й узел.

Поступление ВК трафика на рассматриваемый j - й узел сети со стороны других узлов, заражённых ВК, учитывается значениями булевых коэффициентов: $\alpha_j \in \{0;1\} \forall j \in \{0;N\}$. При наличии вредоносной активности j - го узла $\alpha_j = 1$, при отсутствии таковой $\alpha_j = 0$. При удачном завершении атаки на i - й узел этот узел становится источником вредоносной активности ($\alpha_i \equiv 1$). Так как восстановление узлов в модели сетевой атаки не предусматривается, вредоносная активность узлов сохраняется все время после её возникновения. При алгоритме расчета единичного сценария развития атаки осуществляется процедура многократной реализации текущего случайного выбора узла. При этом с помощью логической процедуры из последующей цепочки событий исключаются те, которые связаны с повторным выбором поражённого внутреннего узла.

Рассматриваемый сценарий характерен для развития случайной атаки, ВК которой не обладает способностью к саморепликации.

Если при дальнейшем развитии модели сценария дополнительно к процессу атаки рассмотреть также процесс активного противодействия атаке системой защиты информации как процесса восстановления работоспособности повреждённых узлов, то величина булевого показателя вредоносной активности восстановленного узла в момент завершения этой операции должна быть обнулена $\alpha_j = 0$. Операция восстановления выполняется в течение определенного интервала времени, которое является случайной величиной, распределённой по заданному статистическому закону.

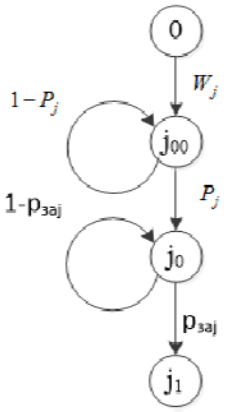

Рис.2. Граф реализации акта завершения атаки на узел:
j_{00} – выбор узла; j_0 – поступление ВК на узел;
j_1 – повреждение узла

Реализация атаки моделируется байесовской трёхзвенной схемой вероятностного выбора [8,9]. В случае выбора определённого узла j (при дополнительном условии $\alpha_j = 0$) с вероятностью W_j разыгрывается исход с поступлением на данный узел ВК с вероятностью P_j, а при успешной реализации предыдущего исхода разыгрывается исход с успешной реализацией захвата узла с вероятностью $p_{заj}$ (рис. 2).

Моделирование вероятностного выбора дискретных исходов трёхзвенной в имитационной модели реализации атаки с переносом ВК на конкретный узел производится методом генерации жребия [10]. В качестве условных вероятностей выбора j - го узла используем параметр W_j, который характеризует относительную по всей сети величину внутреннего трафика, направленного в данный узел. В случае обращения к j - у узлу вероятность P_j поступления на него ВК определяется отношением суммарной интенсивности возможного поступления ВК на данный узел к суммарной интенсивности всего потока событий в сети.

Интенсивность λ_{in} потока событий внутри сети, которые связаны с переносом ВК, определяется с учётом дискретного включения в этот процесс трафика от заражённых узлов. Этот параметр характеризует распределение временных интервалов между возникновением в узлах сети вредоносных кодов и темп развития атаки.

Дополнительно введён параметр, характеризующий распределение времени и темп обработки таких сообщений в узлах $\mu \in \{\mu_1, \dots, \mu_k\}$, *где k – количество узлов в сети.* Модель динамически перестраивает структуру и пересчитывает скорость сетевой атаки по мере захвата узлов, так как поражённые узлы исключаются из множества целей атаки, а количество включаемого вредоносного трафика возрастает с переключением булевых коэффициентов α_j с 0 на 1. Первый фактор снижает скорость выбора цели, а второй – повышает общий темп событий в потоке.

Шкала случайных моментов времени, в которые происходит попытка очередного захвата узла, определяется последовательным суммированием временных интервалов $\Delta\tau$ между событиями попыток захвата. Значения интервалов между событиями распределяются непрерывно $\Delta\tau \in [0;\infty)$ по экспоненциальному закону с переменной интенсивностью $\lambda_{in}(t)$. Таким образом, шкала моментов $t : t_i = t_{i-1} + \Delta\tau_{i-1,i}$ – вычисляется рекурсивно. При успешном завершении атаки к моменту начала успешной попытки захвата некоторого j - ого узла надо добавить случайный интервал времени, затрачиваемого на обработку ВК в узле: $t_{j,i} = t_i + \Delta\tau^{обр}{}_j$. Так определяется случайный момент $t_{j,i}$ времени захвата j - ого узла. Время обработки ВК в j - ом узле распределено непрерывно . по экспоненциальному закону. Таким образом, в некоторые последовательные моменты времени $t_1, t_2, \dots, t_N$, когда происходит захват очередного узла, количество захваченных узлов меняется в последовательности $1,2,\dots,N$. Моделирование случайных значений временных интервалов в модели производим методом обратных функций [10].

Исследование результатов работы имитационной

модели сетевой атаки показывает, что она позволяет определять динамические параметры сетевой атаки, в частности, определять средние скорости захвата узлов ЛВС, определять моменты времени захвата отдельных узлов, исследовать статистические параметры распределения временных характеристик процесса, и т.п.

3. Моделирование динамики случайного процесса противодействия сетевой атаке

Моделирование случайных временных интервалов в операциях реагирования системы защиты на воздействия будем производить по следующей схеме:

$$\Delta T_{СЗИ} = \Delta T_{обн} + \Delta T_{нив},$$

где: $\Delta T_{СЗИ}$ - общая длительность противодействия текущему воздействию; $\Delta T_{обн}$ - время обнаружения угрозы; $\Delta T_{нив}$ - время нивелирования угрозы.

Время обнаружения угрозы считаем распределённым непрерывно и равномерно в некотором интервале $\Delta T_{обн} \in PP\left[\Delta T_{мин}; \Delta T_{макс}\right]$

Время нивелирования угрозы считаем непрерывно распределённым по экспоненциальному закону $F1\left(T < t\right) = 1 - e^{-\mu_{lev} t}$ с параметром μ_{lev} в интервале $\Delta T_{нив} \in \left[0; \infty\right)$.

Эту модель в качестве отдельного модуля реагирования можно включить в рассмотренную выше модель атаки. Сценарий реагирования включается в момент успешного захвата очередного j-ого узла. В момент восстановления, который фиксируется на шкале случайных событий, булев коэффициент обнуляется $\alpha_j = 0$.

Критерием устойчивости системы защиты при реализации этого сценария можно считать выполнение условия, при котором вероятность события, связанного с захватом всех узлов локальной сети за заданный период наблюдения, не превышает некоторого заданного значения: $P_{зах}\left(\ldots, N, T_{набл}, \ldots\right) \le P_{зах}^{доп}$.

Возможна декомпозиция [11,12] модели процесса путём функционального разделения её на модель атаки, которая рассмотрена в предыдущем разделе, и модель противодействия. Модель противодействия или нивелирования угрозы можно представить с использованием математической схемы системы массового обслуживания (СМО) [13]. Схема модели системы защиты на основе СМО, упрощающая решение задачи, требует введения ряда допущений. К числу основных допущений относятся: структурные и процессные унификации. Структурные допущения определяют требования к унификации структуры системы, т.е. унификации узлов и каналов защиты. Процессные допущения требуют однородности потока событий, ограничивая рассмотрение потока событий атакой одного типа при постоянной интенсивности этого потока $\lambda_{cap} = const$. Это значение равно среднему значению скорости, получаемой с использованием модели атаки, где скорость захвата λ_{cap} не является постоянной.

В общем случае систему противодействия можно представить, как систему параллельного резервирования с наличием K каналов обслуживания, что в терминах теории СМО означает схему с накопителем отказов и параллельными каналами нивелирования угроз (рис. 3).

На входе в систему рассматривается ординарный однородный поток отказов, который можно интерпретировать в терминах модели атаки как захват узлов ЛВС с переносом на них ВК.

Для интерпретации динамики процесса изменения состояния системы в этом варианте реализации модели можно использовать динамическую модель «рождения-гибели» [13] узла ЛВС, заражённого ВК.

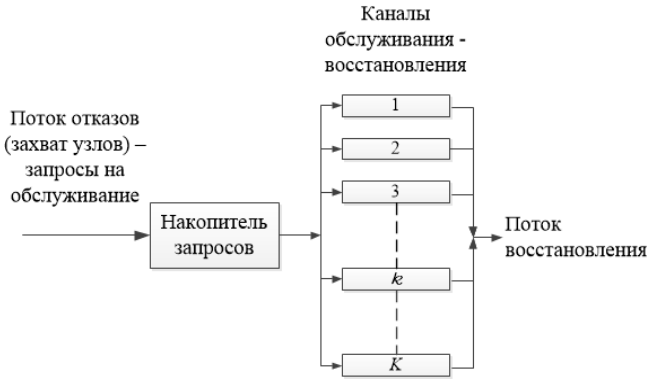

Рис. 3.Схема СМО модели системы противодействия

При этом захват соответствующих узлов в сети интерпретируем как поток событий появления ВК в узлах сети (или отказ узла), а нивелирование угрозы путём обработки ВК в узле будем интерпретировать как восстановление работоспособности узла (рис. 4).

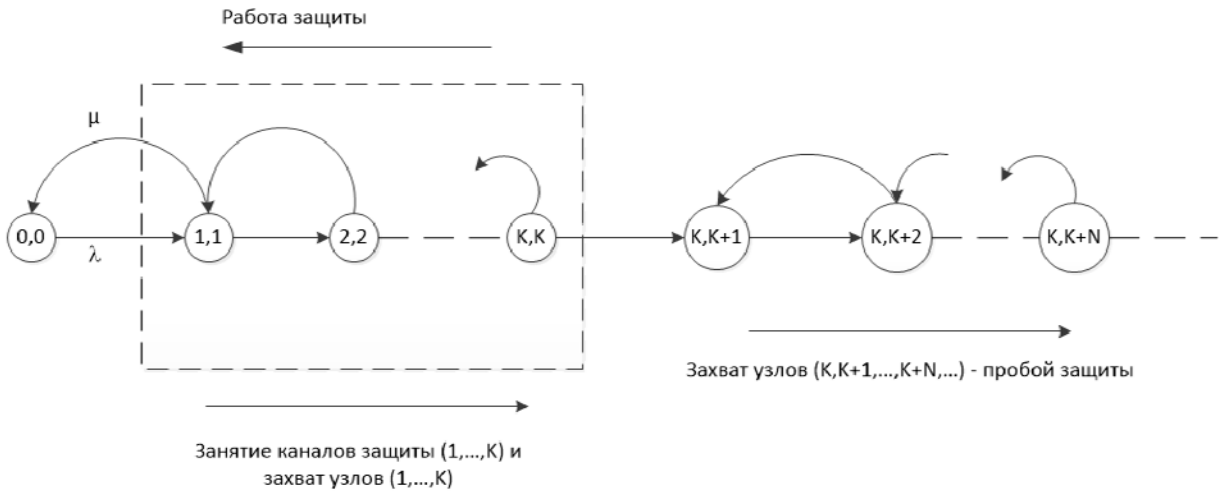

Рис. 4. Модель рождения - гибели ВК в узлах ЛВС

На рис 4 представлена двухиндексная разметка состояний системы, где первый индекс показывает количество задействованных каналов, а второй – количество захваченных узлов, причём в целях упрощения количество узлов считаем неограниченным, а количество каналов – конечным. Для больших сетевых структур это адекватное упрощение.

При исследовании рассматриваемой модели случайного процесса возникновения отказов в распределённой автоматизированной информационной системе с последующим восстановлением основное внимание направлено на характер динамики количества отказов и числа каналов, занятых обслуживанием неисправностей.

При рассмотрении моделируемого процесса выделяем две группы последовательно фиксируемых фактов, которые формируют потоки рассматриваемых событий: поток отказов и поток восстановлений. В потоке отказов число отказов в системе с каждым событием в моменты времени t_{cap}^{i} увеличивается на единицу: $N_{cap} = N_{cap} + 1$, а в потоке восстановлений в моменты времени t_{ex}^{i}, наоборот, уменьшается на единицу: $N_{cap} = N_{cap} - 1$. Таким образом, число отказов в системе меняется разнонаправленно в потоках этих событий, которые чередуются случайным образом во времени.

Таким образом, в рамках рассматриваемой схемы процесса интерес представляет динамика количества захваченных узлов в моменты времени t_{cap}^{i} и t_{ex}^{i}. Процесс по числу захваченных узлов $N_{cap}\left(t_i\right)$ представляет дискретный случайный процесс, имеющий колебательный разнонаправленный характер. Основной задачей моделирования этого процесса является задача построения единой упорядоченной шкалы времени событий t_i путем объединения двух не пересекающихся множеств моментов времени t_{cap}^{i} и t_{ex}^{i}: $t = t_{cap} \cup t_{ex}$ и формирования упорядоченной по возрастанию объединённой последовательности.

Чтобы построить модель этого процесса, надо представить имитационную модель случайных моментов времени наступления рассматриваемых событий, шкала которых строится на моделировании временных интервалов, случайные значения которых распределены по некоторым известным статистическим законам. Интенсивность потока отказов λ_{cap} согласно правилам декомпозиции общей модели получаем, исследуя динамические параметры модели атаки (раздел 1), принимая в качестве него средний параметр интенсивности потока событий, связанного с успешным захватом узлов. Усреднённое значение этого параметра можно получить по результатам прогона имитационной модели атаки.

Упорядоченную по возрастанию последовательность случайных моментов времени захвата узлов ЛВС ВК моделируем, представляя интервалы между событиями захвата как случайные числа $\Delta\tau_{cap}^{i-1,i}$, распределённые непрерывно в диапазоне $[0;\infty)$ по экспоненциальному закону с параметром λ_{cap}. Моделируем эти числа методом обратных функций.

Поток случайных событий появления отказов – ординарный, т.е. представляет упорядоченную во времени последовательность: события появления отказов строго следуют один за другим. Случайные моменты времени потока отказов вычисляются рекурсивным алгоритмом. Время возникновения *i*-ого отказа вычисляется по формуле $t_{cap}^{i} = t_{cap}^{i-1} + \Delta\tau_{cap}^{i-1,i}$. Узлы захватываются последовательно в эти моменты времени. Сразу же, без задержек, в момент успешного захвата узлов начинается процесс восстановления их работоспособности в любом свободном канале, или ожидание обслуживания при занятости всех каналов.

Но поток случайных событий восстановления в общем случае не является упорядоченной во времени последовательностью. Случайные моменты времени потока восстановлений для *i*-ого отказа определяются по формуле: $t_{ex}^{i} = t_{cap}^{i} + \Delta t_{del}^{i} + \Delta T_{СЗИ}^{i}$. Моменты времени восстановления *i*-ого отказа наступают в случайные моменты времени после момента времени появления *i*-ого отказа в системе через промежуток времени, значение которого случайно. Этот интервал является временем существования *i*-ого отказа в системе, которое определяется суммой случайных промежутков времени ожидания восстановления Δt_{del}^{i} и, соответственно, процесса восстановления $\Delta T_{СЗИ}^{i}$.

Процессы по моментам времени t_{cap}^{i} и t_{ex}^{i} характеризуются как случайные, дискретные и аддитивно-накопительные. Такого типа процессы также можно охарактеризовать как рекуррентные, поскольку в них каждое текущее значение последовательно на каждом шаге вычисляется через предыдущие значения процесса. Это хорошо иллюстрируется представленным далее описанием алгоритма расчёта значений процесса.

В общем случае последовательность случайных моментов времени восстановления отказов t_{ex}^{i} не является упорядоченной по возрастанию при наличии более одного канала обслуживания $\left(N_{ch} > 1\right)$, т.к. имеет место параллельное, без задержек, обслуживание поступающих отказов в свободных каналах. Последовательность t_{ex}^{i} является упорядоченной, только если число каналов равно единице $\left(N_{ch} = 1\right)$.

При наличии свободных каналов обслуживания при появлении очередного отказа, т.е. при условии: $N_{cap}\left(t_{cap}^{i}\right) \le N_{ch}$ – каждый отказ без задержек $\left(\Delta t_{del}^{i} = 0\right)$ поступает на обслуживание в свободный канал. Если в момент поступления очередного отказа все каналы обслуживания заняты $\left(N_{cap}\left(t_{cap}^{i}\right) \ge N_{ch}\right)$, то возникает ситуация возможного ожидания обслуживания, когда $\Delta t_{del}^{i} = t_{ex}^{j} - t_{cap}^{i} \ne 0$, $t_{ex}^{j}\left(t_{ex}^{j} > t_{cap}^{i}\right)$ – ближайший момент времени к моменту поступления очередного отказа t_{cap}^{i}, когда выполняется условие $N_{cap}\left(t_{ex}^{j}\right) = N_{ch}$, т.е. освобождается один из каналов обслуживания.

Модель процесса, таким образом, представляет трёхместный кортеж [14] случайных последовательностей: $\left(t_i, N_{capi}, p_i\right)$, где p_i – признак типа события (отказ или восстановление).

Алгоритм имитационного моделирования является рекурсивным, усложнённым рассмотренной выше логикой определения временных интервалов и процедурой упорядочения последовательности моментов времени t_i. Стартовые операции алгоритма:

1- расчёт начинается заданием начальных значений: $t_0 = t_{cap}^0 = 0$ – начальный момент времени, $N_{cap0} = 0$ – начальное состояние системы;

2- вычисляются время первого события и количество отказов в этот момент (тип события – поступление первого отказа $p_1 = 1$): $t_1 = t_{cap}^1 = t_{cap}^0 + \Delta\tau_{cap}^{0,1}$, $N_{cap1} = N_{cap0} + 1 = 1$, где $\Delta\tau_{cap}^{0,1}$ – моделированное методом обратных функций случайное значение временного интервала между событиями потока отказов;

3- вычисляется время второго события (тип события – восстановление первого отказа $p_2 = 2$) при условии, что отказ приходит в свободную систему обслуживания (каналы свободны $\Delta t_{del}^1 = 0$) и количество отказов в системе в этот момент времени: $t_2 = t_{ex}^1 = t_{cap}^1 + \Delta t_{del}^1 + \Delta T_{szi}^1$, $N_{cap2} = N_{cap1} - 1 = 0$. Здесь ΔT_{szi}^1 – моделированное методом обратных функций случайное значение временного интервала, затрачиваемого на восстановление первого отказа.

Далее процедура повторяется заданное количество раз рекурсивно, используя полученные стартовые параметры. Количество шагов процедуры N равно заданному числу наблюдаемых событий в потоке отказов. Поэтому суммарное количество событий в наблюдаемом процессе – длина последовательностей кортежа – составит $2N$, т. к. каждому событию потока отказов соответствует событие его восстановления.

Укрупнённая до процедурного уровня схема алгоритма представлена на рис. 5. На схеме алгоритма в цикле выделены две операции и три процедуры:

1- операция вычисления момента времени, поступившего в систему текущего события типа «отказ»;

2- процедура вставки текущего события типа «отказ» с получением упорядоченных последовательностей кортежа для текущего состояния рекуррентного процесса;

3- процедура определения времени ожидания обслуживания поступившего текущего отказа;

4- операция вычисления момента восстановления текущего отказа;

5- процедура вставки момента времени, сопряженного с поступившим отказом события типа «восстановление» с получением упорядоченных последовательностей кортежа для текущего состояния рекуррентного процесса.

Предложенная имитационная дискретно-событийная модель описывает динамику случайного дискретного процесса противодействия угрозе сетевой атаки со стороны подсистемы защиты в составе автоматизированной информационной системы как системы резервирования с отказами-восстановлениями.

Рис. 5. Фрагмент логической схемы управления процессом в модели СМО

Можно управлять процессом обработки ВК в узлах в модели СМО двумя способами: изменять скорость обработки и использовать параллельные процессы, моделируя их числом параллельных каналов в схеме СМО, регулируя, таким образом, производительность автоматизированной подсистемы защиты от ВК.

4. Результаты имитационного моделирования процессов атаки и защиты

В проведённом исследовании модели сетевой атаки рассматривались сетевые структуры 3-х типов, представленных на рис. 6: сеть 1-го типа и два варианта сети 2-го типа.

Сеть 1-го типа представляет сеть со структурой типа “звезда”, имеющая один центральный узел, к которому, как к коммутатору, подключено 20 оконечных узлов. Сеть 2-го типа в первом варианте представляет сеть с одним центральным узлом, двумя промежуточными узлами, представляющими коммутаторы, к каждому из которых подключено 9 оконечных узлов.

Сеть 2-го типа во втором варианте имеет один центральный узел и четыре промежуточных узла-коммутатора, к каждому из них подключено 4 оконечных узла. Общее количество узлов в структурах трёх сетей составляет в этом случае 21. Это позволяет увидеть наличие влияния структурных особенностей на динамические характеристики процесса сетевой атаки.

Расчёты проводились при параметрах, указанных в таблице 1.

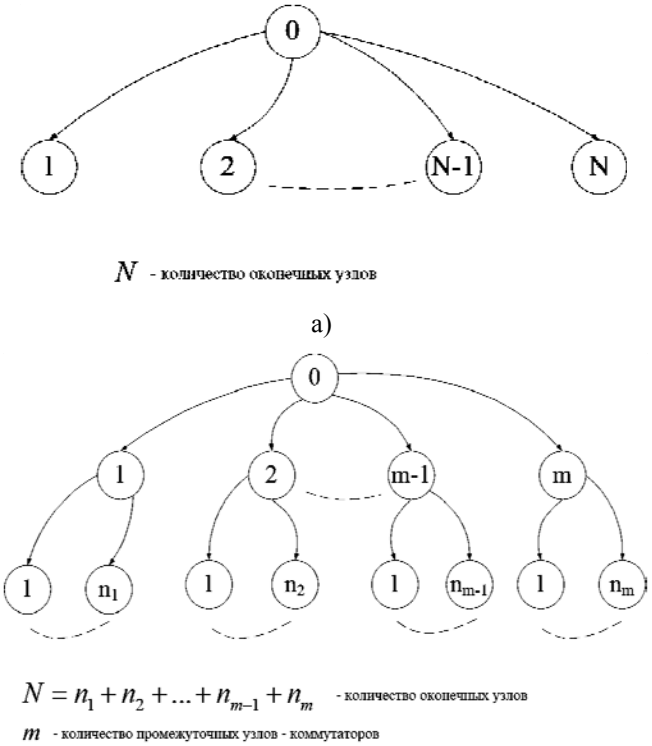

Рис. 6. Структуры локальной сети:
а) сеть с одним центральным узлом (коммутатором), соединённым по схеме звезда с группой оконечных узлов;
б) сеть с одним центральным узлом, группой промежуточных узлов (коммутаторов), соединённых с отдельными группами оконечных узлов

Таблица 1

Название параметра	Ед. изм.	Значение
Интенсивность поступления ВК на вход сети	c^{-1}	0,03
Интенсивность обработки маршрута в сети	c^{-1}	0,07
Интенсивность обработки в узлах сети	c^{-1}	0,05
Относительная частота появления ВК во входящем трафике	-	0,45
Эффективность сетевого экрана на входе в сеть	-	0,75
Отношение внутреннего трафика к внешнему	-	1,25

При имитационном моделировании случайного процесса атаки с захватом узлов ЛВС в качестве упрощающего допущения мы использовали усреднённые статистически характеристики исследуемых процессов (трафик, объёмы файлов, интенсивности потоков событий и т.п.).

При обсуждении приёма декомпозиции с применением модели подсистемы защиты по схеме СМО были введены дополнительные допущения. Каждое допущение, с одной стороны, снижает точность модели, но, с другой стороны, позволяет абстрагироваться от многочисленных несущественных особенностей. Вопрос относительно адекватности такого подхода пока оставим открытым.

На рис. 7 представлены графики зависимости средних затрат времени от относительной доли захваченных узлов для сетей 3-видов, полученные на выборках объёмом 500 значений.

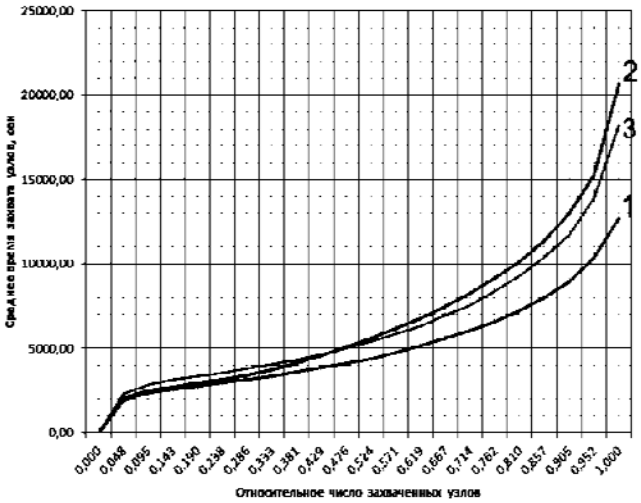

Рис. 7. Средние затраты времени на захват узлов: 1 – сеть 1-го типа, 21 узел; 2 – сеть 2-го типа, 2 узла-коммутатора, 9 узлов в хабе, 21 узел всего; 3 – сеть 2-го типа, 4 узла-коммутатора, 4 узла в хабе, 21 узел всего.

На графиках показаны тренды сценариев случайных рекуррентных процессов, в которых осуществляется последовательное поражение узлов сетевых структур автоматизированных информационных систем. Случайные последовательности захваченных узлов, формируемые при каждой единичной реализации атаки, представляют уникальный сценарий развития атаки. Это иллюстрируют графики 2-ух отдельных единичных траекторий развития событий в пространстве состояний рассматриваемого 1-го варианта сети (рис 8).

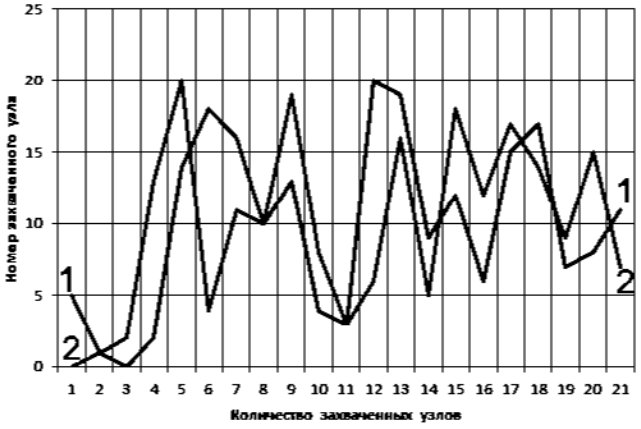

Рис. 8. Траектории захвата узлов:
траектории 1 и 2 – единичные случайные процессы

В этом процессе текущее состояние связано с последовательностью захваченных в процессе сетевой атаки узлов.

Гистограммы (рис. 9) распределения случайных интервалов времени между успешными захватами узлов показывают, что распределение носит экспоненциальный характер со средним значением интервала $\Delta\tau_{ср} \approx 400c$, что даёт оценку параметра $\lambda_{сар} \approx 0,0025c^{-1}$.

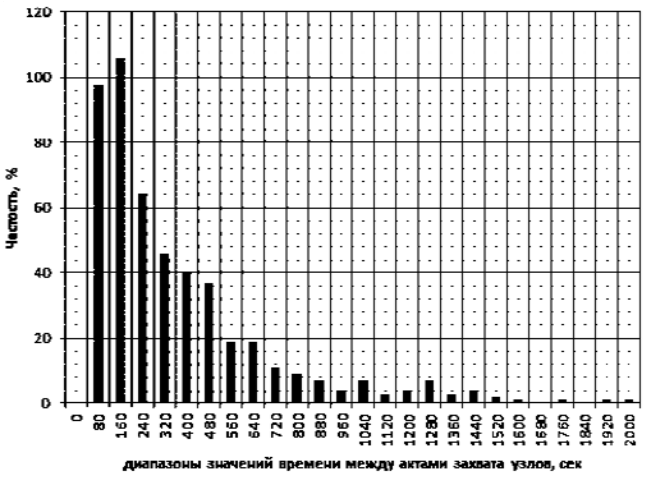

Рис. 9. Гистограмма интервалов времени между событиями атаки

Моделирование вероятности возникновения угрозы ВК на узле по распределению Пуассона с параметром интенсивности λ_{cap} по формуле [10]:

$$P_{угр} = \frac{\left(\lambda_{cap} \bullet T\right)^K}{K!} e^{-\lambda_{cap} \bullet T}$$

показывает, что период времени, при котором имеет место максимальная вероятность (при $\lambda_{cap} \approx 0,0025 c^{-1}$) возникновения угрозы на одном узле ($K = 1$), составляет $T \approx 400 c$. Это время в данном примере следует отвести под операцию устранения угрозы $T = \Delta T_{СЗИ}$.

Вероятность устранения угрозы за данный период времени можно определить по формуле:

$$P_{устр} = \frac{\frac{\left[\mu \bullet \left(T - \Delta T_{обн}\right)\right]^K}{K!}}{\sum_{m=0}^{m=K} \frac{\left[\mu \bullet \left(T - \Delta T_{обн}\right)\right]^m}{m!}}.$$

Оценка по этой формуле для рассматриваемого примера показывает, что вероятность устранения, превосходящая 98%, достигается при $\Delta T_{обн} < 60 c$ и средней скорости устранения угрозы $\mu > 0,15 c^{-1}$.

Оцениваемая скорость обработки высока, она составляет на одно восстановление работоспособности примерно около 7 с. Если включить в оценку также время обнаружения, то общее время на обработку одной проблемы не должно превышать 70 с (точность такой оценки не установлена).

Исследовать картину динамики процесса защиты более адекватно можно путём прогона имитационной модели подсистемы защиты, рассмотренной в предыдущем разделе. Рассмотрим некоторые результаты имитационного моделирования системы с отказами – восстановлениями параллельного резервирования отказов с 5-ю каналами обеспечения восстановления возникающих отказов. Интенсивность стохастического процесса обработки отказов принималась постоянной $\mu_{lev} = 1/400 = 0,0025 c^{-1}$, а интенсивность стохастического процесса потока отказов – переменной, в соответствии с вариантом $\lambda_{cap} = \{0,00125; 0,0025; 0,005; 0,01\} c^{-1}$.

Графики единичных траекторий рекуррентного случайного процесса изменения значений количества отказов в ограниченном диапазоне наблюдаемых событий (от 0 до 150 событий) представлены на рис. 10.

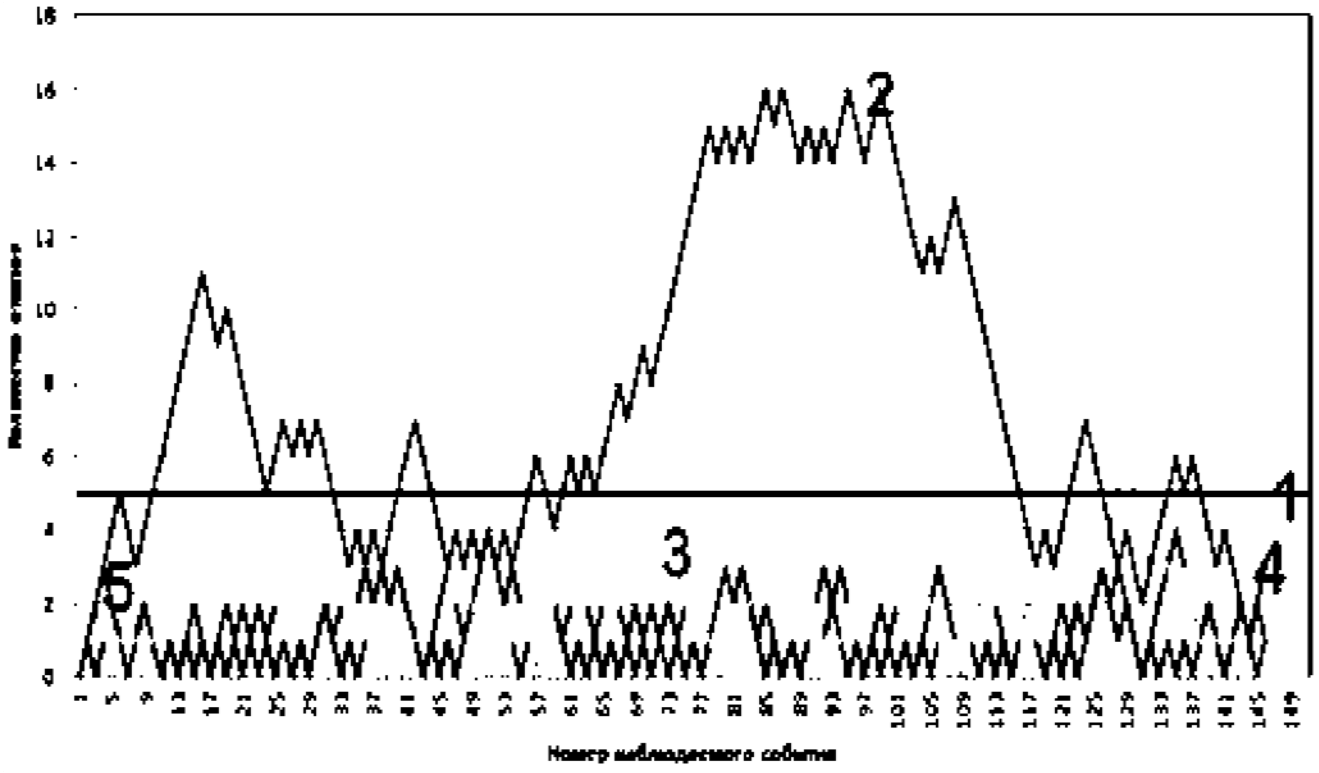

Рис. 10. Траектории единичных сценариев случайного процесса динамики отказов:1 – Число каналов обслуживания; 2 - траектория при интенсивности атаки 0,01 c^{-1}; 3 - траектория при интенсивности атаки 0,005 c^{-1}; 4 - траектория при интенсивности атаки 0,0025 c^{-1}; 5 - траектория при интенсивности атаки 0,00125 c^{-1}.

Траектории на представленном графике соответствуют различным интенсивностям потока отказов из вариантов. Видно, что при двукратном превышении данной интенсивности над интенсивностью процесса восстановления наблюдается устойчивая картина превышения числа возникающих в процессе отказов количества задействованных в системе каналов обслуживания.

Предварительное рассмотрение статистики наблюдаемого процесса при фиксируемых параметрах интенсивности потока отказов по варианту на объёме 40 тыс. значений показывает, что распределение частоты наблюдаемых событий по количеству отказов, попадающих в карманы наблюдаемого диапазона значений распределения, которые указаны в таблице 3, даёт показанное на рисунке 11 распределение частости (частоты) по диапазонам.

Графики показывают, что максимум частости наблюдаемых значений смещается вправо по диапазону наблюдаемых значений при увеличении интенсивности потока отказов, что означает наличие прогнозируемой тенденции возрастания количества отказов в потоке в рассматриваемом случае.

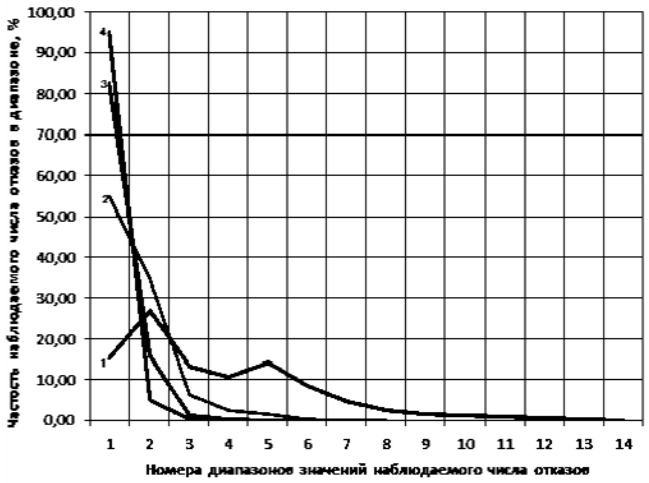

Рис. 11. Распределения частости наблюдаемого числа отказов в карманах диапазона наблюдаемых значений: 1 - траектория при интенсивности атаки 0,01 $с^{-1}$; 2 - траектория при интенсивности атаки 0,005 $с^{-1}$; 3 - траектория при интенсивности атаки 0,0025 $с^{-1}$; 4 - траектория при интенсивности атаки 0,00125 $с^{-1}$

Таблица 3

№ диапазона	1	2	3	4	5	6	7	8	9
Карманы диапазона, кол.отказов	0-2	2-4	4-5	5-6	6-8	8-10	10-12	12-14	14-16

Эту тенденцию можно представить в несколько ином свете. Если ввести в рассмотрение частость превышения в процессе количеством отказов количества каналов как эмпирическую оценку вероятности «пробоя защиты», то её зависимость от значения интенсивности потока отказов по данным статистического моделирования представлена на рис. 12.

График, представленный на рисунке 12, хорошо показывает влияние скорости потока отказов на надёжность защиты при заданных параметрах её производительности. Вероятность отказов начинает тем больше возрастать, чем больше превышение интенсивности потока отказов над интенсивностью потока восстановлений.

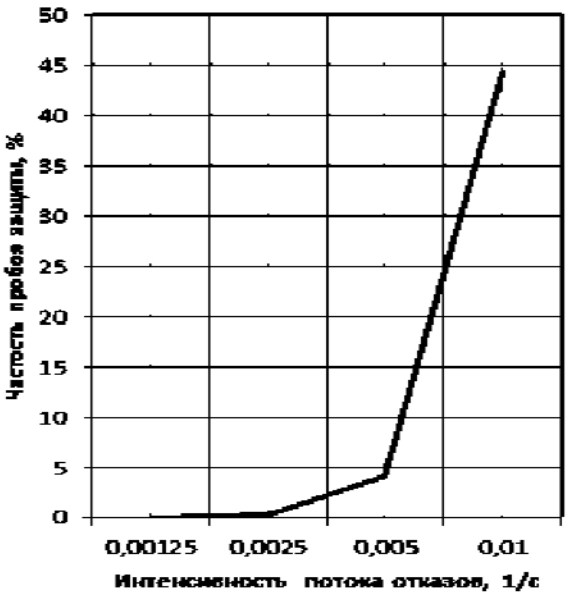

Рис. 12. Зависимость частости «пробоя защиты» от интенсивности потока отказов

5. Выводы по результатам работы

Рассмотренные в работе имитационные модели используют только временные параметры нестационарного дискретного случайного процесса, событиями которого являются акты выхода из строя или восстановления работоспособности элементов некоторой информационной системы, имеющей сетевую структуру. Результат моделирования представляет, по сути, некоторый журнал наблюдений, фиксирующий последовательно, когда и какие события происходят.

Представленный алгоритм позволяет моделировать стохастические динамические процессы в сложноорганизованных системах, которые имеют распределённые разветвлённые сетевые структуры.

С помощью рассмотренных моделей можно проводить статистические испытания таких систем методом имитационного математического моделирования, исследовать статистические параметры случайных процессов в стохастических системах такого типа.

Результаты моделирования позволяют получать необходимые динамические параметры исследуемых процессов. Это могут быть как скоростные характеристики развития процессов сетевой атаки, так и необходимая скорость противодействия ей со стороны автоматизированной системы защиты, роль которой заключается в предотвращении или минимизации рисков последствий компьютерных инцидентов.

Для определения скоростных характеристик необходимо исследование зависимостей темпов сетевых атак от факторов структурной организации, вероятностных

параметров развития атаки и эффективности штатных средств локальной защиты, а также исследование динамических и вероятностных показателей взаимодействия в случайном процессе потоков отказов и восстановлений. При проектировании автоматизированных подсистем защиты от внешних атак это является актуальной задачей.

Отдельно можно обсудить решение задач определения показателей надёжности с использованием предложенных в работе алгоритмов. К числу важных свойств надёжности подсистем защиты можно отнести, например, свойство устойчивости системы противодействия угрозам информационной безопасности.

Если рассматривать свойство надёжности подсистемы защиты в процессе функционирования по обеспечению безопасности информационной системы в контексте предложенного сценария, то в некоторых задачах ситуация, когда в моделируемом процессе количество отказов в системе в моменты событий появления очередных отказов превышает количество имеющихся в подсистеме защиты каналов обслуживания, может рассматриваться как критическая. Такой взгляд на проблему защиты может представлять интерес при рассмотрении атак на автоматизированные информационные системы типа «отказ в обслуживании» (DOS, DDOS, Flood-атаки, и т.п.) [15]. В эти моменты времени происходит «пробой защиты», когда в последующий период времени возникающие в системе отказы могут накапливаться. В эти периоды подсистема защиты перегружена обработкой отказов, накопленных в очереди.

Если рассмотреть этот алгоритм как модель изменения во времени количества свободных каналов, то она имитирует случайный процесс противодействия атаке типа «отказ в обслуживании», при отражении которой критичным является наличие в автоматизированной информационной системе свободных каналов обслуживания.

Занятие каналов снижает скорость работы автоматизированной информационной системы, поэтому количество каналов обслуживания и скорость обработки запросов превращается в фактор устойчивости системы к резкому повышению нагрузки.

В других задачах в качестве критичной может быть рассмотрена ситуация, когда происходит захват некоторого критического количества или всех узлов ЛВС, например, сетевой полевой структуры управления объектами критичной информационной инфраструктуры. Такую критическую ситуацию можно интерпретировать как отказ.

Если алгоритм представляет модель динамики захвата узлов функционирующей сетевой структуры, то минимизация количества отказов, которая сочетается с оперативным восстановлением работоспособного состояния, представляет фактор надёжности функционирования критичной информационной инфраструктуры.

Определение конкретного критерия отказа в моделируемом процессе зависит, таким образом, от вида той системы, к описанию которой применяется модель.

Литература

1. ГОСТ Р 27.013-2019 Надежность в технике. Методы оценки показателей безотказности.
2. Казарин О. В. , Шубинский И. Б. Основы информационной безопасности: надежность и безопасность программного обеспечения: учеб.пособие для СПО (Серия: Профессиональное образование). — М.: Издательство «Юрайт», 2019. — 342 с.
3. Чекал Е. Г. , Чичев А. А. Надежность информационных систем: учебное пособие: в 2 ч. – Ульяновск: УлГУ, 2012. – 118 с.
4. Ерохин С. Д. , Петухов А. Н. , Пилюгин П. Л. Управление безопасностью критических информационных инфраструктур. – М.: Научно-техническое издательство «Горячая линия - Телеком», 2021. – 240 с.
5. Петухов А. Н. , Гуснин С. Ю. Эталонная модель безопасности критических информационных инфраструктур./ ст. в журнале (материалы конференции). – СПб: Изд-во СПбГЭУ (ЛЭТИ им. В.И. Ульянова) // Международная конференция по мягким вычислениям и измерениям, 2019. - Том 1. - С. 243-246.
6. Горбачев И. Е. , Глухов А. П. Моделирование процессов нарушения информационной безопасности критической инфраструктуры. – СПб: СПб. ФИЦ РАН, Ж. «Труды СПИРАН», 2015. - Вып. 1(38). - С. 112-135.
7. Лебедев В. В. , Лозовецкий В. В. , Комаров Е. Г. Динамическая дискретно-событийная имитационная модель распространения атаки на узлы связи транспортной компьютерной сети /Lebedev V.V., Lozovetsky V.V., Komarov E.G. Dynamic discrete-event simulation model of the propagation of an attack on communication nodes of a transport computer network) // Научный информационный сборник ВИНИТИ РАН. Транспорт: наука, техника, управление («Transport: science, equipment, management scientific» information collection). – 2021. - №1. - С. 26 – 33.
8. Тулупьев А. Л. , Сироткин А. В. , Николенко С. И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. – СПб: Издательство С-Петербургского университета, 2009. — 400 с.
9. Корниенко А.А., Никитин А.Б., Диасамидзе С.В., Кузьменкова Е.Ю. Моделирование компьютерных атак на распределенную информационную систему. – СПб: ПГУПС, журнал «Известия Петербургского университета путей сообщения» (Proceedings of Petersburg Transport University), 2018/4. - С. 613 – 628.
10. Гельгор А. Л. , Горлов А. И. , Попов Е. А. Методы моделирования случайных величин и случайных процессов: уч. пос. – СПб: Изд-во ПГПУ, 2012. — 217 с.
11. Плотников С. А. , Семенов Д. М. , Фрадков А. Л. Математическое моделирование систем управления. / Уч. пос. – СПб: Университет ИТМО, 2021. — 194 с.
12. Павловский Ю. Н.. Проблема декомпозиции в математическом моделировании. – М.: ВЦ АН СССР// Математическое моделирование. (Тем. раздел: вычислительные алгоритмы и методы). – 1991. - Том 3. - №6. - С. 93 – 122.

13. Хинчин А. Я. Работы по математической теории массового обслуживания. – М.: Либроком, 2010. — 240 с.

14. Математический энциклопедический словарь. / Гл. ред. Прохоров Ю.В. – М.: Научное издательство «Большая Российская Энциклопедия», 1995. — 847 с.

15. Аграновский А. В. , Хади Р. А. . Новый подход к защите информации – системы обнаружения компьютерных угроз. – Ростов на Дону: ФГНУ НИИ «Спецвузавтоматика», информационный бюллетень «JetInfo», № 04(167)/2007. - С. 2-22.

Сведения об авторах

Лозовецкий Вячеслав Владимирович, д.т.н., профессор, МГТУ им. Н.Э. Баумана (Мытищинский филиал),
141018, Мытищи ул. Лётная, д.23, кв. 123
Тел. моб. – 8 915 347 48 00
E-mail: lozovetsky@mail.ru

Лебедев Владимир Владимирович, к.т.н., доцент, Российский технологический университет – МИРЭА.
119571, ЦФО, г. Москва, Проспект Вернадского, д. 86
Тел. моб. 8 96 397 237 82
E-mail: voval_matr@mail.ru.

Шукенбаев Айрат Бисенгалеевич, к.т.н., доцент, Российский технологический университет – МИРЭА,
119571, ЦФО, г. Москва, Проспект Вернадского, д. 86.
Тел. моб. 8 916 582 95 78
E-mail: shukenbaev@mail.ru.

Сергущенко Андрей Васильевич, начальник научно-исследовательской лаборатории ФГКУ "12 ЦНИИ" Минобороны России.
Тел моб. 89998298010
E-mail: andser79@yandex.ru.

Архипенко Андрей Валентинович, к.т.н., Сочинский международный инновационный университет
Тел. Моб. 8 953 077 39 70
E-mail:andrei-arhipenko@mail.ru.