DOI: 10.36535/0236-1914-2021-01-5

УДК 681.3.06

ДИНАМИЧЕСКАЯ ДИСКРЕТНО-СОБЫТИЙНАЯ ИМИТАЦИОННАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ АТАКИ НА УЗЛЫ СВЯЗИ ТРАНСПОРТНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Кандидат техн. наук, доцент **Лебедев В.В.**
(Российский технологический университет – МИРЭА)

Доктор техн. наук, профессор **Лозовецкий В.В.,**
доктор техн. наук, профессор **Комаров Е.Г.**
(МГТУ им. Н.Э. Баумана. Мытищинский филиал)

DYNAMIC DISCRETE-EVENT SIMULATION MODEL OF THE PROPAGATION OF AN ATTACK ON COMMUNICATION NODES OF A TRANSPORT COMPUTER NETWORK

Ph. D. (Tech.)**,** Associate Professor **Lebedev V.V.**
(Rossiysky Technology University – MIREA)

Doctor (Tech.), Professor **Lozovetsky V.V.,**
Doctor (Tech.), Professor **Komarov E.G.**
(Moscow State Technical University named after N. Bauman. Mytishchi Branch)

Имитационная модель, стохастический процесс, атака на локальную вычислительную сеть, распространение вредоносного контента по узлам сети, вероятностные параметры случайного процесса, сценарий развития событий в сети, надёжность как устойчивость к распространению атаки.

Simulation model, stochastic process, attack on a local area network, distribution of malicious content over network nodes, probable parameters of a random process, scenario of development of events in the network, reliability as resistance to attack propagation.

Представлен сценарий развития случайного дискретного процесса атаки на локальную вычислительную сеть (ЛВС) с распространением вредоносного контента (ВК), источником которого выступает трафик, содержащийся в отдельных фрагментах ВК. Трафик может быть внешним по отношению к ЛВС или исходить из некоторых узлов. Рассматривается 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. Вероятностный характер имеет поступление ВК на выбранный случайный узел, а также факт успешного завершения атаки на узел в этом случае. Рассматриваемый сценарий характерен для развития случайной атаки ВК, которой не обладает способностью к саморепликации. Подробно разбирается алгоритм имитационной модели данного процесса, обсуждаются некоторые результаты численного моделирования и возможные применения данной модели при решении прикладных задач.

A scenario of the development of a random discrete process of an attack on a local computer network (LAN) with the spread of malicious content (VC), the source of which is the traffic containing in separate VK fragments, is presented. Traffic can be external to the LAN, or originate from some nodes. A sparse random process of VC propagation is considered, which is characterized by random time intervals between VC occurrences at the entrance to the network nodes. The choice of the direction of traffic to network nodes is random. It is probable that a VC arrives at a selected random node, as well as the fact that the attack on a node is successfully completed in this case. The scenario under consideration is typical for the development of a random VC attack, which does not have the ability to self-replicate. The algorithm of the simulation model of this process is analyzed in detail, some results of numerical modeling and possible applications of this model in solving applied problems are discussed.

Исследование устойчивости сетевых структур относительно различных видов несанкционированных воздействий обычно основывается на изучении динамики процессов, на моделях системной динамики, в том числе, адаптированных к сетевым процессам, например, так называемых эпидемиологических моделях [1, 2], или исследовании вероятностных характеристик надёжности рассматриваемых сетевых структур [3].

Анализ опыта применения таких моделей свидетельствует о возможности удовлетворительного описания усреднённой динамики таких процессов, при условии обеспечения точности определения параметров моделей, которые существенно зависят от особенностей изучаемых сетевых структур и статистики процессов, происходящих в них. Опыт изучения статистики сетевых процессов [4] показывает их значительное разнообразие. Аналогичный вывод даёт исследование современных сетевых структур и их характеристик [5].

Учитывая вышесказанное, определение параметров моделей системной динамики, адекватных исследуемым сетевым структурам и процессам, является предметом экспериментальных исследований в каждом конкретном случае. Эффективным инструментом при проведении подобных исследований выступает имитаци-

онное моделирование [6]. Модели, создаваемые методами имитационного моделирования, дают возможность исследовать сложные системы, учитывать их разнообразные характеристики, включая статистические и структурные. Следует отметить недостаточно подробное описание таких моделей и алгоритмов в современных публикациях, что затрудняет обмен опытом в области разработки и применения имитационных моделей.

Рассматриваемые в данном случае несанкционированные воздействия относятся к виду разрушающих программных воздействий, которые осуществляют несанкционированную реализацию на конкретном вычислительном ресурсе разрушающего программного кода или размещение иного вредоносного контента (ВК), компрометирующего ресурс. Эти угрозы потенциально возникают при передаче вредоносного кода или контента на отдельные узлы сети в составе трафика, которым обмениваются узлы сети.

В представленной ниже имитационной модели компьютерной атаки на локальную вычислительную сеть рассматривается разреженный стохастический процесс, при котором интервалы времени между возникновениями сообщений на входе системы больше времени их обработки в системе. Статистика таких процессов подчиняется экспоненциальному или гиперэкспоненциальному закону [7].

Сценарий рассматриваемого процесса включает следующие последовательности случайных событий: последовательность событий поступления вредоносных кодов в сеть, актов поступления этих кодов на отдельные узлы и актов успешного завершения атак на выбранные узлы. В случае поступления разрушительного программного кода разыгрывается выбор целевого узла сети, а затем акта успешного захвата данного узла. В случае успеха данный узел включается в набор захваченных узлов, входя в пул распространителей вредоносного кода. Атака продолжается до полного захвата всех узлов.

Дескриптивная модель процесса

В основу модели положим представление об интенсивности атаки на сеть, которую можно связать с интенсивностью дискретного потока сообщений ρ на входной сетевой 0-ой узел, частотой попыток реализации угрозы атаки π_o, показателем надёжности защиты сетевого экрана $p_{зсэ}$. Интенсивность входного потока, содержащего потенциальную угрозу для узлов сети, представим в виде формулы:

$$\lambda^0 = \left(1 - p_{\text{ЗСЭ}}\right)\rho\pi_0 \qquad (1)$$

Этот параметр характеризует статистическое распределение временных интервалов между приходом в сеть вредоносных кодов или ВК, что позволяет определять случайные затраты времени на полное завершение реализации атаки в сети.

Дополнительно необходимо ввести параметры, характеризующие распределение времени обработки таких сообщений в отдельных узлах системы $\{\mu_1,\ldots,\mu_k\}$, обслуживание сообщений может включать затраты времени на маршрутизацию и передачу, а также на обработку. Частота событий внутри локальной сети может отличаться, возможны два различных сценария. В первом случае трафик, содержащий ВК, может просто перенаправляться 0-ым узлом в нисходящем потоке из внешней сети к другим узлам внутренней сети. В этом варианте плотность потока будет определяться по формуле (1). Во втором случае, когда 0-ой узел и другие узлы сети сами становятся источниками ВК, плотность потока событий будет увеличиваться в зависимости от величины внутреннего трафика:

$$\lambda^{\text{in}} = \lambda^0\left(1 + f_{\text{tr}}\right), \qquad (2)$$

где f_{tr} – коэффициент внутреннего трафика.

Взаимодействие узлов сети между собой представим орграфом (рис. 1.)

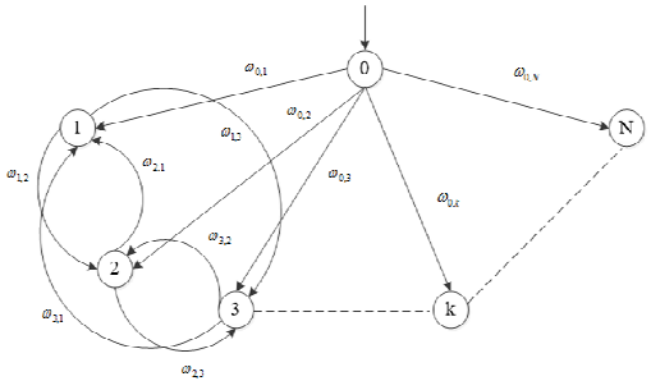


Рис. 1. Схема графа связи между узлами локальной сети

Частоту $\omega_{i,j}$ входящих обращений из i - го узла в j - й узел определяем, нормируя трафик между отдельными узлами на суммы трафика в столбцах:

$$\omega_{i,j} = \frac{t_{i,j}}{\sum_{i=0}^{N} t_{i,j}}, \qquad (3)$$

где $t_{i,j}$ – величина трафика, направленного из i - го узла в смежный с ним j - й узел; $\sum_{i=0}^{N} t_{i,j} = t_j$ – величина суммарного трафика, входящего в j - й узел; $\omega_{i,j}$ – относительная частота взаимодействия i - го узла со смежными ему j - ми узлами.

Частоту $\omega_{i,j}$ входящих обращений из i - го узла в j - й узел определяем, нормируя трафик между отдельными узлами на суммы трафика в столбцах:

$$\omega_{i,j} = \frac{t_{i,j}}{\sum_{i=0}^{N} t_{i,j}}, \qquad (3)$$

где $t_{i,j}$ – величина трафика, направленного из i - го узла в смежный с ним j - й узел; $\sum_{i=0}^{N} t_{i,j} = t_j$ – величина суммарного трафика, входящего в j - й узел; $\omega_{i,j}$ – относительная частота взаимодействия i - го узла со смежными ему j - ми узлами.

Моделирование акта выбора узла в имитационной модели производится методом реализации жребия, схема которого представлена на рис. 2.

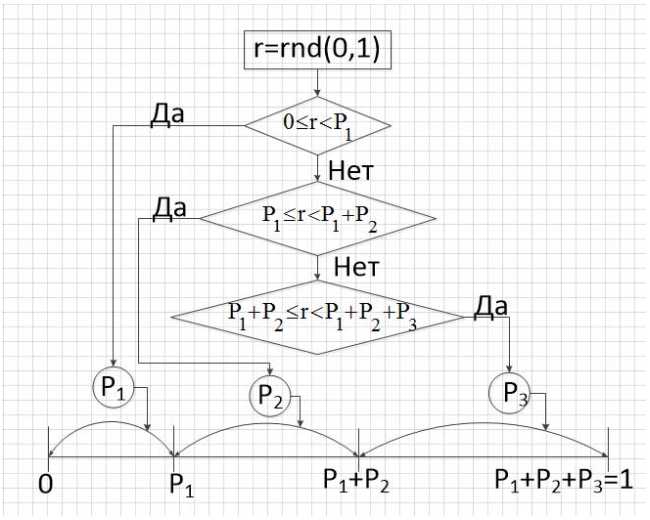


Рис. 2. Моделирование акта выбора узла в имитационной модели

В качестве условных вероятностей выбора j - го узла на рис. 2 вместо P_1, P_2, P_3 используем параметр, который характеризует относительную по всей сети величину внутреннего трафика, направленного в данный узел:

$$W_j = \frac{\sum_{i=0}^{N} t_{i,j}}{\sum_{j=0}^{N}\sum_{i=0}^{N} t_{i,j}}, \qquad (4)$$

где $t_{\text{in}} = \sum_{j=0}^{N} t_j = \sum_{j=0}^{N}\sum_{i=0}^{N} t_{i,j}$ – суммарный внутренний трафик, входящий в узлы.

В случае выбора j - го узла граф реализации акта завершения атаки на узел может быть представлен схемой на рис. 3.

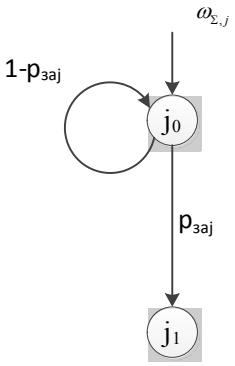


Рис.3. Граф реализации акта завершения атаки на узел

Поступление вредоносного трафика на рассматриваемый j - й узел сети со стороны других узлов можно в общем виде представить формулой:

$$t_j = \sum_{i=0}^{N} \alpha_i t_{i,j}, \qquad (5)$$

где $\alpha_i \in \{0;1\} \forall i \in \{0;N\}$ – булево значение наличия вредоносной активности узла.

При наличии вредоносной активности j - го узла $\alpha_j = 1$, при отсутствии таковой $\alpha_j = 0$. При удачном завершении атаки на i - й узел он становится источником вредоносной активности ($\alpha_i \equiv 1$). Восстановление узлов в данной модели не рассматривается, вредоносная активность узлов сохраняется все время после её возникновения. При многократной реализации текущего выбора узла следует исключить из рассмотрения события, связанные с повторным выбором поражённого внутреннего узла, применяя логическую процедуру исключения этого узла из последующей цепочки событий.

Интенсивность дискретного потока событий, возможно, связанных с переносом вредоносного воздействия, определим формулой:

$$\lambda^{\text{in}} = \lambda^0 + \frac{1}{m_{\text{f}}}\sum_{j=0}^{N}\sum_{i=0}^{N}\alpha_i t_{i,j} = \\ = \lambda^0\left(1 + \frac{\rho_{\text{in}}}{\rho\left(1-p_{\text{ЗСЭ}}\right)}\sum_{j=0}^{N} W_j \sum_{i=0}^{N}\alpha_i \omega_{i,j}\right), \qquad (6)$$

где m_{f} – средний по трафику объём файла; $\rho_{\text{in}} = \frac{t_{\text{in}}}{m_{\text{f}}}$ – интенсивность дискретного потока сообщений внутри сети.

Коэффициент внутреннего трафика при этом представляется формулой:

$$f_{\text{tr}} = \frac{\rho_{\text{in}}}{\rho\left(1-p_{\text{ЗСЭ}}\right)}\sum_{j=0}^{N} W_j \sum_{i=0}^{N}\alpha_i \omega_{i,j} \qquad (7)$$

Данная модель позволяет динамически перестраивать граф атаки на узлы сети по мере захвата узлов, так как количество включаемого вредоносного трафика возрастает с переключением булевых коэффициентов α_i с 0 на 1.

В случае обращения к j - у узлу вероятность поступления на него ВК можно оценить формулой:

$$P_j = \frac{\lambda^0 W_j + \rho_j \sum_{i=0}^{N}\alpha_i \omega_{i,j}}{\rho W_j + \rho_j \sum_{i=0}^{N}\omega_{i,j}} = \\ = \frac{\lambda^0 W_j + \rho_j \sum_{i=0}^{N}\alpha_i \omega_{i,j}}{\rho W_j + \rho_j} = \frac{\lambda^0 + \rho_{\text{in}}\sum_{i=0}^{N}\alpha_i \omega_{i,j}}{\rho + \rho_{\text{in}}}, \qquad (8)$$

где $\rho_j = \frac{t_j}{m_{\text{f}}}$ – интенсивность дискретного потока сообщений на данный узел, причём: $\sum_{i=0}^{N}\omega_{i,j} = 1$; $\sum_{j=0}^{N} W_j = 1$; $\rho_j = \rho_{\text{in}} W_j$.

Событие, связанное с приходом вредоносного трафика на узел в имитационной модели разыгрываем с вероятностью, определённой по формуле (8), тем же методом, что и при выборе узла, реализуя выбор между двумя событиями в соответствии с табл. 1.

Таблица 1

Дискретное распределение для ВК

Событие	Вероятность
Поступление ВК на j - ый узел	P_j
Отсутствие поступления ВК на j - ый узел	$1-P_j$

Вероятность завершения атаки с поражением узла разыгрываем подобным образом, реализуя выбор по табл. 2.

Таблица 2

Дискретное распределение по завершению атаки

Событие	Вероятность
Успешное завершение атаки на j - ый узел	$p_{заj}$
Нет завершения атаки на j - ый узел	$1-p_{заj}$

Значения вероятностей в таблицах 1 и 2 могут, в общем случае, различаться по узлам, поэтому их распределение по узлам может быть представлено векторно: $\{\ldots,P_j,\ldots\};\{\ldots,p_{заj},\ldots\}, j=0,1,2,\ldots,N$.

Соответственно, исход, не связанный с поражением j - го узла, будет равен $1-p_{заj}$. Таким образом, рассмотренные исходы составляют полную группу несовместных событий, что позволяет имитировать исходы в модели, используя схему реализации «жребия».

Плотность потока событий, которые связаны с передачей ВК формулой (6), будет расти при подключении внутреннего вредоносного трафика. Этот рост ограничивается диапазоном: $\lambda^{\text{in}} \in \left[\lambda^0;\lambda^0\left(1+\frac{\rho_{\text{in}}}{\rho(1-p_{зсэ})\pi_0}\right)\right]$. С другой стороны, снижение числа не захваченных узлов будет вести к снижению общей скорости захвата, поскольку при этом снижается относительная частота обращений к узлам, остающимся не захваченными.

Сначала коэффициент внутреннего трафика равен $f_{\text{tr}}=0$, потому что узлы не захвачены ВК, и значения булевых коэффициентов равны $\alpha_i=0\,\forall i\in\{0,1,\ldots,N\}$, $\lambda^{\text{in}}=\lambda^0$.

С плотностью потока событий в модели будет связана шкала времени фиксации событий, т.е. актов успешного завершения атаки на узел сети. В эту временную оценку включается момент времени завершения успешной атаки на узел, который равен сумме момента времени начала атаки с продолжительностью обработки в узлах.

Моменты начала атаки моделируются как накопительная шкала, суммирующая случайные промежутки времени возникновения в системе случайных обращений к текущему узлу и фиксирующая события при успешном завершении атаки. Случайные промежутки возникновения событий моделируем как числа, распределённые по экспоненциальному закону с параметром λ^{in}, используя метод обратных функций по формуле:

$$\Delta t=\frac{1}{\lambda^{\text{in}}}ln\left(\frac{1}{1-r}\right),$$

где r – случайное число, распределённое по равномерному закону (РР(0,1)). Сгенерированная последовательность $\{r_1,r_2,\ldots r_k\}$ порождает, таким образом, последовательность временных интервалов $\{\Delta t_1,\Delta t_2,\ldots,\Delta t_k\}$. Накопительное суммирование элементов этой последовательности определяет шкалу случайных моментов времени событий, которые связаны с началом потенциальных атак: $t_k=\sum_{i=1}^{k}\Delta t_i$. Случайные продолжительности обработки блоков ВК при успешном завершении атаки моделируются аналогично по экспоненциальному закону:

$$\Delta t_O=\frac{1}{\mu}ln\left(\frac{1}{1-r}\right),$$

где μ – интенсивность обработки, равная отношению среднего за определённый период трафика к среднему объёму передаваемого файла или блока данных.

При прогоне модели реализуется единичный вариант развития случайного процесса, в результате которого фиксируется журнал регистрации событий, связанных с захватом узлов локальной сети (табл.3).

Таблица 3

Журнал регистрации событий

№ события, связанного с успешной реализацией атаки	Номер захваченного узла сети	Время начала успешной атаки	Время обработки вредоносного сообщения в узле	Время завершения атаки, $t^{\kappa}{}_j$
1	n_1	t_{n_1}	Δt_{on_1}	$t_{n_1}+\Delta t_{on_1}$
2	n_2	t_{n_2}	Δt_{on_2}	$t_{n_1}+\Delta t_{on_2}$
…	…	…	…	…
k	n_k	t_{n_k}	Δt_{on_k}	$t_{n_k}+\Delta t_{on_k}$
…	…	…	…	…
N	n_N	t_{n_N}	Δt_{on_N}	$t_{n_N}+\Delta t_{on_N}$

Используя данные таких журналов, полученные при многократном прогоне модели, можно определить статистические характеристики динамического процесса изменения состояния системы, в частности, средние характеристики времени захвата узлов сети (табл.4).

Таблица 4

Результаты статистической обработки данных имитационной модели

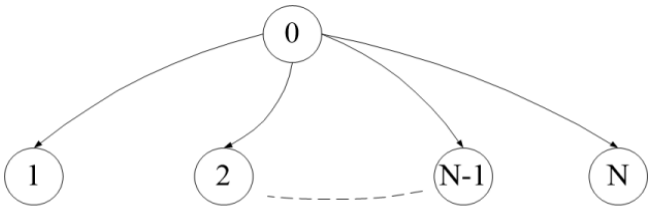
Количество захваченных узлов ко времени фиксации события, n	1	2	…	k	…	N
Средняя оценка времени фиксации события, $t^{\kappa}{}_j$	$\boldsymbol{t}^{\kappa}{}_1$	$\boldsymbol{t}^{\kappa}{}_2$	…	$\boldsymbol{t}^{\kappa}{}_k$	…	$\boldsymbol{t}^{\kappa}{}_N$
Относительное количество захваченных узлов, a	$\frac{1}{N}$	$\frac{2}{N}$	…	$\frac{k}{N}$	…	1

Если рассматривать общую последовательность попыток реализации атаки на узлы как акты испытаний системы, а исходы, которые сопровождаются успешным завершением атак, как акт частичного отказа или повреждения, то эти данные могут служить для оценки отказоустойчивости системы по отношению к данному виду угрозы. В этом контексте время захвата всех узлов сети можно интерпретировать как наработку на отказ. Эти результаты представляют интерес с точки зрения исследования факторов, характеризующих надёжность автоматизированной информационной системы.

Данные табл.4 могут быть использованы для построения объясняющей регрессионной модели, например коэффициентов моделей системной динамики. Данные табл. 3, получаемые при многократном прогоне модели, представляют интерес при исследовании статистических характеристик процесса, например таких, как время полного захвата узлов сети.

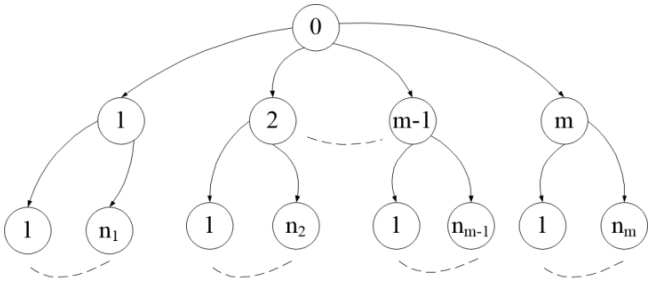
В модели могут быть рассмотрены различные сетевые структуры, поскольку структура определяется видом матрицы частости обращений между узлами сети (рис. 2). При испытании модели рассматривались структуры, представленные на рис. 4.

При разработке программы целесообразно разрабатывать отдельно два блока. Один блок должен обеспечивать конструирование требуемой сетевой структуры, характеристики которой по отношению к рассматриваемому типу атак предстоит исследовать. Второй блок получает параметры исследуемой сетевой структуры из первого блока и выполняет прогон имитационной модели развития сценария сетевой атаки в этой сети.



N - количество оконечных узлов

а)



$N = n_1 + n_2 + \ldots + n_{m-1} + n_m$ - количество оконечных узлов

m - количество промежуточных узлов - коммутаторов

б)

Рис. 4. 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

Поскольку вариантов сетевых структур много: от различных регулярных структур до сетей со случайными структурами, то первый блок может предоставлять разнообразные возможности и алгоритмы для моделирования всего разнообразия актуальных сетевых структур.

При проведении расчётов по рассмотренному алгоритму оценивались два варианта сети: сеть 1-го типа и сеть 2-го типа.

Расчёты проводились при следующих параметрах (табл. 5).

Таблица 5

Исходные данные для расчётов

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

Сеть первого типа представляет сеть со структурой типа “звезда”, имеющая один центральный узел, к которому, как к коммутатору, подключено 20 оконечных узлов. Результаты расчёта затрат времени на захват узлов сети этого типа представлены на рис. 5. Графики представляют полигональные диаграммы затрат времени на последовательный захват узлов в сети при случайной реализации единичных сценариев, в ходе которых формируются разные последовательности узлов.

Рис. 5. Затраты времени на захват узлов в сети первого типа: ряды 1-11 – случайные реализации процесса; ряд 12 – средние затраты времени

График средних затрат времени усредняет результаты всех единичных реализаций. Результат демонстрирует значительную вариативность временных параметров процесса.

Сеть второго типа представляет сеть с одним центральным узлом, двумя связанными с ним узлами, представляющими коммутаторы, к которым подключены оконечные узлы. Количество оконечных узлов, подключаемых к каждому коммутатору, составляет 9. Таким образом, общее количество узлов этой сети равно 21, также как и в сети 1-го типа. Результаты расчёта затрат времени на захват узлов сети этого типа представлен на рис.6.

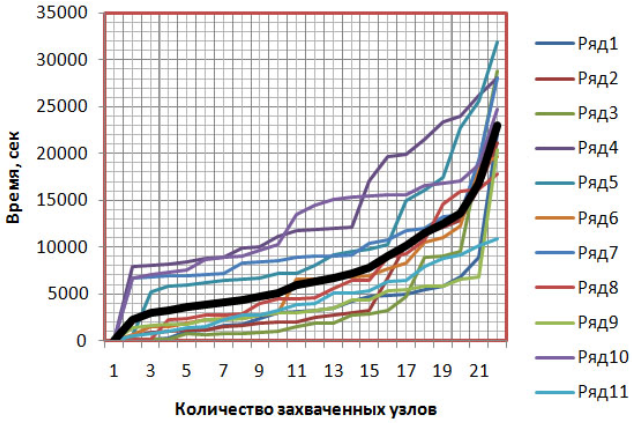


Рис. 6. Затраты времени на захват узлов в сети второго типа: ряды 1-11 – случайные реализации процесса; ряд 12 – средние затраты времени

Графики аналогично графикам рис. 5 представляют полигональные диаграммы затрат времени на последовательный захват узлов в сети при случайной реализации единичных сценариев, в ходе которых формируются разные последовательности узлов. График средних затрат времени усредняет результаты всех единичных реализаций. Результаты расчёта также отличаются высокой вариативностью. Флуктуации случайных единичных реализаций значительно сглаживаются при увеличении объёмов выборки.

Сети похожи, но сеть 2-го типа отличается более разветвлённой структурой. Графики, представленные на рис. 5 и 6, построены на данных одиннадцати случайных реализаций процесса и свидетельствуют о высокой дискриминантивности результатов расчётов.

На рис. 7 представлены графики зависимости средних затрат времени от относительной доли захваченных узлов, полученные на выборке объёмом 500 значений.

Рис. 7. Средние затраты времени на захват узлов: ряд 1 – сеть 1-го типа; ряд 2– сеть 2-го типа

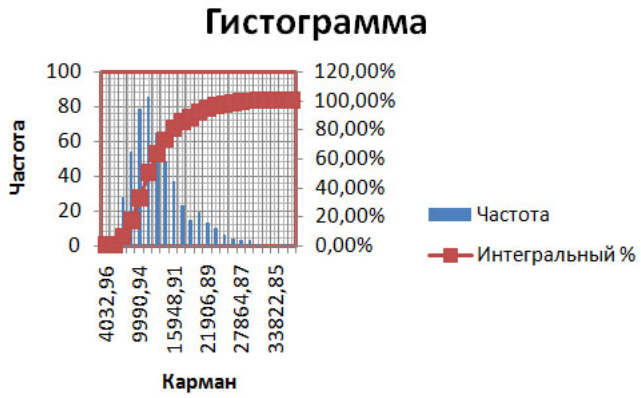
Случайные последовательности узлов, формируемые при каждой единичной реализации атаки, представляют уникальный сценарий развития единичных атак, прочерчивая траекторию развития событий в пространстве состояний рассматриваемой сети (рис 8).

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

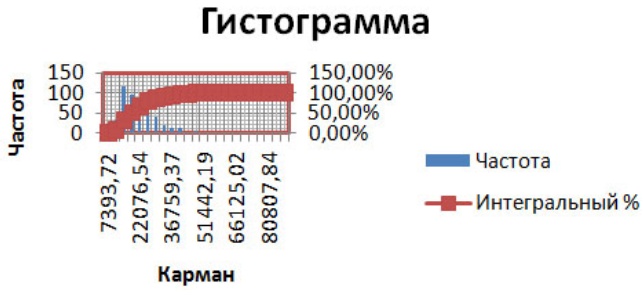
Представленная имитационная модель реализует случайный дискретный процесс распространения ВК в сети.

Расчёты по данной модели позволяют получать и обрабатывать статистический материал, касающийся, в частности, законов распределения времени захвата узлов сети, вероятности захвата отдельных узлов сети на каждом шаге и т. п..

На рис. 9 представлены гистограммы распределений для сетей 1-го и 2-го типа. Рассматриваемые значения времени характеризуют стойкость сети к данному виду атак.



а)



б)

Рис. 9. Распределение времени на захват всех узлов сети: *а*) – сеть 1-го типа; *б*) – сеть 2-го типа

Выводы

1. Предложена имитационная модель развития случайного дискретного процесса атаки на ЛВС (локальную вычислительную сеть) с распространением вредоносного ВК.

2. Численное моделирование с её использованием проведено для сети с одним центральным узлом, соединённым по схеме «звезда» с группой оконечных узлов и сети с одним центральным узлом, группой промежуточных узлов, соединённых с отдельными группами оконечных узлов.

3. Результаты расчётов с использованием разработанного алгоритма имитационной модели случайного дискретного процесса распространения ВК в сети свидетельствуют о значительной вариативности временных параметров процесса и о возможности обработки статистического материала, касающегося распределения времени захвата узлов сети.

4. Предложенная модель может рассматриваться как инструмент исследования случайных дискретных процессов в сетях, влияния структурных и вероятностных факторов на устойчивость сети к атакам данного типа и может быть применена при решении прикладных задач.

Литература

1. Аграновский А.В., Тихонов А.Н., Скуратов А.К., Хади Р.А.. Математическая модель угроз безопасности автоматизированных систем в компьютерной сети RUNNET. – [Электронный ресурс]. URL: http://kniga.seluk.ru/k-bezopasnost/1138246-1-razdel-kompyuterno-telekommunikacionnoe-obespechenie-primeneniya-informacionnih-tehnologiy-obrazovanii-matematichesk.php. 2014. – 4с.

2. Roberts M.G., Heesterbeek JAP. Mathematical models in epidemiology. – Oxford: EOLSS Publishers Ltd, In JA. Filar (Ed.) Mathematical Models, 2004. – 17 с.

3. Бутузов В.В. Информационные риски флуд-атакуемых компьютерных систем: Монография/ В.В. Бутузов, М.В. Бурса. А.Г. Остапенко. А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга». 2015. – 160 с.

4. Степанов С.Н. Основы телетрафика мультисервисных сетей. — М.: Эко-Трендз, 2010. – 392 с.

5. Евин И.А. Введение в теорию сложных сетей. – М.: компьютерные исследования и моделирование, Т. 2 № 2, 2010. – с. 121-141.

6. Марголис Н.Ю. Имитационное моделирование. – Томск: Издательский Дом Томского государственного университета, 2015. – 130с.

7. Кравцов А.О., Привалов А.А., Ракк М.А. Модель процесса передачи пакетов данных в сети mpls-tp в условиях компьютерных атак при редкоследующем входящем потоке. – М. // Автоматизация процессов управления. - 2019. - № 2 (56) – С. 44-52.

Сведения об авторах

Лебедев Владимир Владимирович, к.т.н., доцент Российского технологического университета – МИРЭА,
Москва, ул. Стромынка, 20
E-mail: voval_matr@mail.ru.

Лозовецкий Вячеслав Владимирович, д.т.н., профессор Московского государственного технического университета им. Н.Э. Баумана (Мытищинский филиал),
Мытищи 5, ул.1-ая Институтская, д. 1.
Тел. 8-915-347-48-00
E-mail: lozovetsky@mail.ru.

Комаров Евгений Геннадиевич - д.т.н., профессор Московского государственного технического университета им. Н.Э.Баумана (Мытищинский филиал),
Мытищи 5, 1-ая Институтская ул., д. 1.
Тел. 8-917-563-47-59
E-mail: fuzzykom@gmail.com.