Научная статья
УДК 004.056
https://doi.org/10.24143/2072-9502-2022-2-66-75

Метод Монте-Карло для оценки устойчивости функционирования объекта информатизации в условиях массированных компьютерных атак

Владислав Александрович Воеводин

Национальный исследовательский университет «Московский институт электронной техники», Москва, Зеленоград, Россия, vva541@mail.ru

Аннотация. Методы математической статистики и теории вероятностей глубоко изучены и могут успешно применяться как средство оценки устойчивости функционирования объектов информатизации (ОИ) в штатных условиях их применения. Штатные условия позволяют добыть репрезентативную описательную статистику, оценить соответствующие вероятностные характеристики и применить методы теории вероятностей. Обеспечение надежности функционирования ОИ в штатных условиях обеспечивается результативным эксплуатационным прикрытием. Однако для массированных компьютерных атак (МКА) динамика поведения ОИ и развитие обстановки непредсказуемы, а сами события относятся к редким, что не позволяет корректно применять названные выше методы. Значимость и новизна исследования заключаются в положительной оценке применимости метода Монте-Карло для оценки живучести восстанавливаемого ОИ, подверженного МКА и обладающего временной избыточностью (восстанавливаемостью). Оценка живучести ОИ рассматривается с точки зрения необходимости внедрения методологии страхования рисков информационной безопасности, связанных с МКА. Приводятся постановка задачи, алгоритм моделирования, примеры решения, на основании которых можно рекомендовать метод Монте-Карло для решения поставленной задачи. Приводятся укрупненные этапы процедуры статистического моделирования, описано решение актуальной задачи по оценке устойчивости ОИ для условий МКА. Полученные частные выводы могут представлять интерес для планирования дальнейших научных исследований в направлении совершенствования процессов выработки решений по обеспечению устойчивости функционирования ОИ в условиях целенаправленных агрессивных воздействий. Приводится практический пример статистического моделирования с учетом возможных сценариев нанесения МКА и интерпретации результатов моделирования.

Ключевые слова: метод Монте-Карло, массированная компьютерная атака, живучесть, восстановление работоспособности, объект информатизации, страхование рисков

Для цитирования: *Воеводин В. А.* Метод Монте-Карло для оценки устойчивости функционирования объекта информатизации в условиях массированных компьютерных атак // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. № 2. С. 66–75. https://doi.org/10.24143/2072-9502-2022-2-66-75.

Original article

Monte Carlo method for estimating informatization object stable functioning in conditions of massive computer attacks

Vladislav A. Voevodin

National Research University of Electronic Technology, Moscow, Zelenograd, Russia, vva541@mail.ru

Abstract. Methods of mathematical statistics and probability theory are deeply studied and can be successfully used as a means of assessing the stability of the functioning of informatization objects (OI) in the normal conditions of its application. The standard conditions allow us to obtain representative descriptive statistics, evaluate the corresponding probabilistic characteristics and apply the methods of probability theory. Ensuring the reliability of the functioning of OI in normal conditions is provided by effective operational cover. However, for massive computer attacks (MCA), the dynamics of OI behavior and the development of the situation are unpredictable, and the events themselves are rare, which does not allow the above methods to be correctly applied. The significance and novelty of the study lies in

the positive assessment of the applicability of the Monte Carlo method for assessing the survivability of the restored OI, which is subject to MCA and has temporary redundancy (recoverability). Assessing OI survivability is considered from the point of view of the need to implement a methodology for ensuring the risks of information security associated with MCA. The statement of the problem, the modeling algorithm, and solution examples are given, on the basis of which it is possible to recommend the Monte Carlo method for solving the set problem. The enlarged stages of the statistical modeling procedure are given, the solution of the actual problem of assessing OI stability for MCA conditions is described. The obtained partial conclusions may be of interest for planning further scientific research in the direction of improving the processes of decision making to ensure the sustainability of the functioning of OI in conditions of targeted aggressive influences. A case of statistical modeling is given, taking into account possible scenarios for applying MCA and interpreting the simulation results.

Keywords: Monte Carlo method, massive computer attack, survivability, recovery, object of informatization, risk insurance

For citation: Voevodin V. A. Monte Carlo method for estimating informatization object stable functioning in conditions of massive computer attacks. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics.* 2022;2:66-75. (In Russ.) https://doi.org/10.24143/2072-9502-2022-2-66-75.

Введение

Развитие цифровых технологий и усложнение информационной инфраструктуры сопровождается ростом количества киберпреступлений [1, 2]. Вопросы, связанные с управлением рисками искажения информации, простоя деловых процессов в результате совершения киберпреступлений, приобретают все большую актуальность. Сведения о динамике киберпреступлений приведены в [1, 2]. Реализация киберпреступлений возможна посредством осуществления компьютерных атак, в том числе массированных. Вопросы тестирования и мониторинга защищенности информационных систем от компьютерных атак рассматривались в работах В. В. Кульбы, С. И. Макаренко, И. И. Лившица, А. С. Маркова и др. Отдельные результаты исследований приведены в [3–7].

В рамках настоящей статьи под компьютерной атакой (КА) понимается целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств [8]. Страхование перечисленных рисков, связанных с реализацией КА, выглядит разумным способом обеспечения информационной безопасности (ИБ), в основе которого лежит экономический фактор [9]. Сама по себе процедура страхования рисков ИБ предполагает участие, помимо страхователя и страховщика, аудитора ИБ. Задача аудитора – дать объективную и независимую оценку информационных рисков и подготовить исходные данные для обоснования принимаемого решения по их страхованию. При этом аудитор должен обладать достоверными, научно обоснованными методиками, которые позволили бы оценить устойчивость функционирования страхуемого объекта информатизации (ОИ) в условиях массированных компьютерных атак (МКА). Важным условием является то, что в силу доказанной достоверности и полноты аудиторского заключения ему доверяют одновременно и заказчик аудита (страхователь), и страховщик. Общие вопросы организации и проведения аудита ИБ рассмотрены в работах [3–8, 10].

Постановка задачи исследования

Задача оценки устойчивости функционирования ОИ, как и технических средств обработки информации, входящих в его состав и обладающих временной избыточностью, формулируется следующим образом.

Определены исходные данные, характеризующие:

– интенсивность МКА, $\mathsf{I} = \{\boldsymbol{F}, n\}$, где $\boldsymbol{F}$ – множество функций распределения случайных интервалов времени h_i, до очередной i-й КА, $\boldsymbol{F} = \{F_i(t)\}$, где $F_i(t)$ – функция распределения случайного h_i интервала времени до i-й КА, $i = 1, 2, \ldots, n$, n – число КА в составе МКА;

– надежность функционирования ОИ в штатных условиях и защищенность ОИ от КА (варьируемые характеристики) – $u = \{T_н, P\}$, где $T_н$ – наработка между отказами в штатных условиях эксплуатации; P – множество значений вероятностей поражения ОИ в результате МКА, $P = \{p_i\}$, где p_i – вероятность поражения ОИ при i-й КА. Оценка вероятностей p_i осуществляется экспертным путем в соответствии с подходами, приведенными в [11–13], методиками, опубликованными в [14, 15], и зарегистрированными Роспатентом программными средствами [16, 17];

– способность ОИ к восстановлению работоспособности (варьируемые характеристики), $r = \{T_в, G\}$, где $T_в = \{\mathsf{t}_{вi}^{н}, \mathsf{t}_{вi}^{в}\}$ – множество прогнозируемых интервалов времени восстановления; G – множество функций распределения случайных интервалов времени восстановления ОИ после i-й атаки; $G = \{G_i(t)\}$, $i = 1, 2, \ldots, n$, n – число атак; $\mathsf{t}_{вi}^{н}$ – оценка нижней границы времени восстановления ОИ после i-й атаки, $\mathsf{t}_{вi}^{в}$ – оценка верхней границы времени восстановления ОИ после i-й КА. Оценка параметров $\{\mathsf{t}_{вi}^{н}, \mathsf{t}_{вi}^{в}\}$ осуществляется с помощью методики, опубликованной в [14], и программных средств [16, 17].

Требуется разработать общую процедуру и исследовать частные случаи определения наименьше-

го значения v_m функции устойчивости ОИ на заданном интервале времени нанесения МКА (0, T]:

$$\nu_m = \inf_{t \in (0,T]} \nu(t, \lambda, r, u),$$

где t – текущий момент времени оценки функции живучести; λ, r, u – исходные данные (см. предыдущий раздел).

Функция устойчивости ОИ на заданном интервале времени (0, T], согласно [18], будет иметь вид

$$\nu(t, \lambda, r, u) = K_г(u, r)\varphi(t, \lambda, r, u), \qquad (1)$$

где $K_г$ – коэффициент готовности ОИ в штатных условиях эксплуатации; $\varphi(t, \lambda, r, u)$ – функция живучести ОИ в условиях МКА.

Алгоритмы *точных аналитических моделей* основаны на общей процедуре оценивания коэффициента готовности, в основе которых лежат математические модели известных функций распределения $F_i(t)$ и $G_i(t)$, приведенных в [18]. Значение коэффициента готовности ОИ определяется с помощью соотношения, приведенного в [19]:

$$K_г = T_н (T_н + T_в)^{-1},$$

где $T_н$, $T_в$ определяются на основании статистики, полученной в условиях штатной эксплуатации ОИ. Для большинства случаев $K_г \geq 0{,}99$, а наименьшее значение функции живучести $\psi_m << K_г$, поэтому $K_г$ в формуле (1) можно пренебречь, тогда функция устойчивости упрощается и сводится к

$$\eta_m \approx \psi_m = \varphi(t, \lambda, r, u).$$

Задача решается в два этапа:

1) определение оператора A: $\psi(t) = A\{\boldsymbol{F}, \boldsymbol{G}, P, n\}$;

2) определение минимума функционала $\varphi_m = \inf_{t \in (0,t]} \varphi(t)$.

Результаты экспериментальных исследований позволяют утверждать, что наиболее сложным является первый этап, в ходе которого рассматриваются различные виды операторов A и осуществляется выбор подходящего:

– оператора A_0, определяемого при произвольных законах распределения элементов множеств $\{F_i(t)\}$ и $\{G_i(t)\}$ и различных $\{P_i\}$. В этом случае представляется возможным процесс функционирования ОИ характеризовать как *общий полумарковский*;

– оператора A_1, определяемого при одинаковых законах распределения элементов множеств $\{F_i(t)\}$ и $\{G_i(t)\}$ и равных $\{P_i\} = P$. Процесс функционирования ОИ можно характеризовать как *частный полумарковский*;

– оператора A_2, определяемого при экспоненциальных законах распределения $F(t) = 1 - e^{-\lambda t}$ и $G(t) = 1 - e^{-\mu t}$ и равных $\{P_i\} = P$. В этом случае процесс можно характеризовать как *марковский*;

– оператора A_3, определяемого при однократной КА $n = 1$.

Модели функционирования ОИ в условиях МКА можно разделить на 3 подгруппы:

– точная математическая модель;

– приближенная аналитическая модель;

– статистическая модель, в основу которой положен метод Монте-Карло.

В зависимости от принятой модели строится и сам алгоритм моделирования. Вывод математических моделей для определения A_2, A_3 приведен в [18, 19]. Точные аналитические методы целесообразно использовать при относительно небольшом числе КА, при $n \leq 2$. Это обусловлено тем, что при увеличении числа n для вычисления функции живучести $\psi(t)$ требуются достаточно сложные, громоздкие и трудноинтерпретируемые аналитические выражения.

Алгоритмы *приближенных аналитических моделей* основаны на использовании различных аппроксимирующих зависимостей, упрощающих аналитические выражения для вычисления функций $F_i(t)$, $G_i(t)$ и $\psi(t)$, позволяющие с достаточной, для оценочных суждений, точностью описать усеченные нормальные законы распределения случайных величин η_i и τ_i. Для этого требуется применение законов Эрланга высших порядков.

Алгоритм *статистического моделирования* целесообразно применять при больших значениях n, когда аналитические выражения для отображения $\psi(t)$ имеют громоздкий и трудноинтерпретируемый вид.

Для статистического моделирования каждой j-й реализации $z_j(t)$ случайного процесса $z(t)$ сопоставляется последовательность состояний атакуемого элемента (ОИ), $z_{ij}(t) = z_j(t_i)$, $i = 1, 2, \ldots, m$, определяемых в дискретные моменты времени $t_i = i \times \Delta t$. Значения m вычисляются в соответствии с заданным интервалом времени моделирования [0, T) и единичным интервалом Δt по формуле $m = T / \Delta t$.

С учетом сказанного выше процедура статистического моделирования будет включать следующие укрупненные этапы:

1. Задается число s требуемых реализаций $z_j(t)$ случайного процесса $z(t)$, $i = 1, 2, \ldots, s$.

2. Формируется последовательность моментов времени t_i, $i = 1, 2, \ldots, m$.

3. Определяется последовательность возможных моментов времени атак и восстановлений работоспособности моделируемого элемента:

$$T_{wvj} = \{0, T_{w1j}, T_{v1j}, T_{w2j}, T_{v2j}, \ldots, T_{wnj}, T_{vnj}\},$$

где $T_{w1i} = T_{v(i-1)i} + \eta_{ii}^*$; $T_{v1i} = T_{wii} + \tau_{ii}^*$; $i = 1, 2, \ldots, n$, $T_{v0i} = 0$; n – число КА; η_{ii}^* – i-я реализация случайной величины η, формируемая с помощью датчика случайных чисел в соответствии с выбранным законом распределения $F_i(t)$; τ_{ii}^* – i-я реализация случайной величины τ, формируемая с помощью датчика случайных чисел в соответствии с выбранным законом распределения $G_i(t)$.

4. Для каждой реализации j определяется событие успешности КА в соответствии с условием: если Rnd() > P (где Rnd() – значение датчика случайных чисел на интервале (0, 1), распределенных по заданному закону распределения случайной величины), то атака считается неуспешной.

5. Последовательно формируются реализации $z_j(t) = \{z_{ij}\}$ в силу условий:

$$z_{ij} = 1, \text{ если Rnd()} > P;$$
$$z_{ij} = 1, \text{ если Rnd()} < P \text{ и } T_{v(i-1)j} \le t_i \le T_{wij};$$
$$z_{ij} = 0, \text{ если Rnd()} < P \text{ и } T_{wij} \le t_i \le T_{vij};$$
$$i = 1, 2, \ldots, m.$$

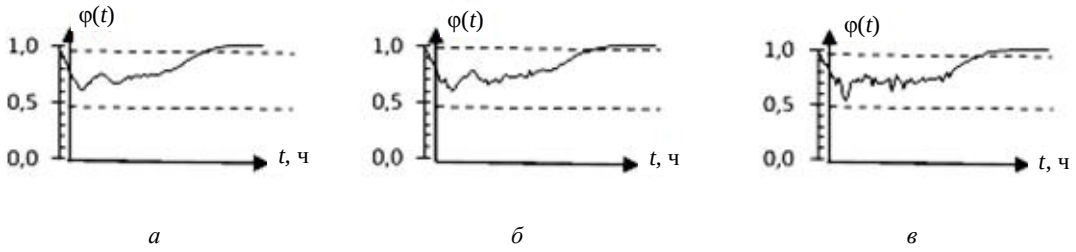
6. Осуществляется суммирование полученных значений соответствующих состояний z_{ij} по всем реализациям и определяется оценка $\varphi^*(t_i)$ значений функции живучести в моменты времени t_i по формуле

$$\varphi^*(t_i) = \frac{1}{s}\sum_{j=1}^{s} z_{ij},$$

где $i = 1, 2, \ldots, m$.

Алгоритм реализован с помощью программы для ЭВМ [20, 21], позволяющей получить функцию живучести ОИ для условий МКА при произвольном количестве воздействий и произвольных законах распределения случайных величин η и τ.

Результаты моделирования в зависимости от числа реализаций приведены на рис. 1, где $\varphi(t)$ – значение функции живучести – безразмерная величина от 0 до 1; t – время, ч.



а *б* *в*

Рис. 1. Вид функций живучести $\varphi(t)$ в зависимости от числа реализаций:
а – 2 000 реализаций; *б* – 500 реализаций; *в* – 100 реализаций

Fig. 1. Type of survivability function depending $\varphi(t)$ on the number of realizations:
а – 2, 000 implementations; *б* - 500 implementations; *в* - 100 implementations

С ростом числа реализаций функция живучести приобретает более сглаженный вид, причем локальные минимумы ее можно наблюдать уже на 500 реализациях (рис. 1, *б*). В результате моделирования появляется возможность определить нижнюю и верхнюю границы времени восстановления объекта МКА, обеспечивающие заданное значение показателя живучести; функцию живучести ОИ в процессе МКА; неблагоприятные интервалы времени, в течение которых функция живучести минимальна или может оказаться ниже требуемой.

Алгоритм решения задачи. Допустим, что страховая компания (страховщик) установила понижающие коэффициенты страхового тарифа по страхованию информационных рисков в зависимости от оценки минимального значения функции живучести φ_m: ($\varphi_m < 0{,}79$; страхование риска ИБ для страховщика убыточно) ($0{,}79 \le \varphi_m < 0{,}8$; $k = 1$); $0{,}8 \le \varphi_m < 0{,}9$; $k = 0{,}7$; $0{,}9 \le \varphi_m < 0{,}95$; $k = 0{,}5$; ($\varphi_m > 0{,}95$; $k = 0{,}45$, причем для обеспечения $\varphi_m > 0{,}95$ требуется значительный ресурс, что убыточно для страхователя), где k – коэффициент снижения страховой премии в зависимости от защищенности ОИ от КА.

Лицо, управляющее рисками ИБ, приняло решение, что рациональным является вариант 2 (φ_m 0,8 ≤ φ_m; $k = 0{,}7$). Руководство ОИ и страховщика для оценки защищенности ОИ от МКА решили обратиться за аудиторским заключением к независимой аудиторской компании, чтобы по итогам аудита (аудиторского заключения) принять решение о целесообразности страхования финансовых рисков, связанных с возможным нарушением непрерывности бизнеса в результате МКА.

Для оценки уровня защищенности от МКА аудиторская компания спланировала эксперимент со статистической моделью, для чего:

– был сформирован и согласован с заказчиками аудита сценарий МКА;

– был изучен план обеспечения непрерывности бизнеса ОИ (План) и получены исходные данные для моделирования.

Характеристики МКА на ОИ (фиксированные переменные):

– прогнозируемое число МКА – 4;

– прогноз интенсивности КА – одна КА в течение 12 ч;

– прогнозируемый период осуществления МКА – 2 сут.

Моменты нанесения КА характеризуются случайными числами h_i, i = 1, 2, 3, 4, распределенными по равномерному закону. Первая и последующие КА осуществляются в случайные моменты времени: $h_1 \in$ ($h_{1н}$ = 0, $h_{1в}$ = 12 ч]; $h_2 \in$ ($h_{2н}$ = 12, $h_{2в}$ = 24 ч]; $h_3 \in$ ($h_{3н}$ = 24, $h_{3в}$ = 36 ч]; $h_4 \in$ ($h_{4н}$ = 36, $h_{4в}$ = 48 ч], где $h_{iн}$, $h_{iв}$ – нижняя и верхняя границы равномерного закона распределения времени i-й КА.

Характеристики плана поддержания непрерывности бизнеса ОИ (управляемые переменные):

– оценка вероятности поражения ОИ P = 0,4;

– согласно плану восстановления непрерывности бизнеса ОИ $t_н$ – минимально возможное время восстановления работоспособности ОИ после КА – составляет 6 ч (0, 25 сут), а максимально допустимое $t_в$ = 12 ч (0,5 сут). Случайная величина t распределена по равномерному закону в пределах нижней – $t_н$ – и верхней – $t_в$ – границ указанного диапазона (варьируемые переменные).

Ограничения: восстановление осуществляется методом сканирования серверного оборудования и рабочих станций с помощью антивируса, удаления вредоносного файла и восстановления пораженных файлов; планом поддержания непрерывности бизнеса предусмотрено, что наименьшее значение функции живучести ОИ не должно опускаться ниже 0,8, т. е. $\varphi_m \geq 0{,}8$.

Требуется установить, удовлетворяют ли заданные характеристики плана восстановления непрерывности бизнеса при заданных характеристиках МКА установленному требованию – ($\varphi_m \geq 0{,}8$, чтобы получить скидочный коэффициент k = 0,7). Если требования не выполняются, то путем корректирования значений варьируемых переменных найти такие их значения, при которых требования выполняются и при этом требуется минимальный ресурс – R_π; подобная постановка задачи приведена в [17]. R_π – требуемый ресурс для реализации π-го плана поддержания непрерывности бизнеса ОИ, $\pi \in P$, P – множество планов поддержания непрерывности бизнеса ОИ, удовлетворяющих условию $0{,}8 \leq \varphi_m \leq 0{,}81$. Ограничение сверху функции живучести ОИ, 0,81, мотивируется тем, что необходимо: а) снизить размерность задачи поиска рационального Плана; б) исключить избыточную ресурсоемкость Плана.

Если значение функции живучести для заданного Плана удовлетворяет требованиям ($0{,}8 \leq \varphi_m \leq 0{,}81$; k = 0,7), то формируется аудиторское заключение о соответствии Плана требованиям. В противном случае задача усложняется и осуществляется поиск рационального варианта Плана. Если функция живучести значительно превосходит требования, то формируется аудиторское заключение об избыточной ресурсоемкости Плана. Если функция живучести меньше требований, то формируется аудиторское заключение о недостаточном уровне защищенности ОИ от МКА.

Для решения задачи был спланирован и проведен эксперимент со статистической моделью поведения ОИ в условиях МКА. Модель была построена средствами Excel. Полученный результат представлен в виде графика (рис. 2).

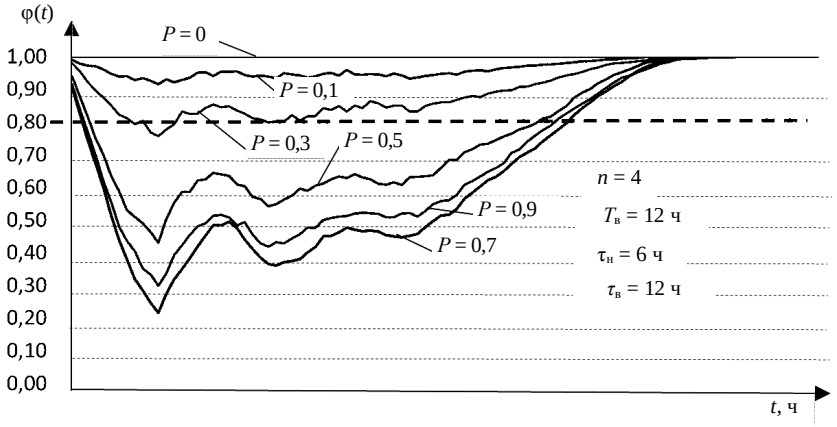


Рис. 2. Изменение функции живучести $\varphi(t)$ в зависимости от вероятности поражения объекта компьютерной атаки при фиксированных исходных данных (усреднено 2 000 реализаций)

Fig. 2. Changing the survivability function depending $\varphi(t)$ on probability of damaging the object of a computer attack at fixed initial data (averaged over 2, 000 realizations)

На рис. 2 представлены графики функций живучести ОИ в условиях МКА. Задача поиска решается графически. Так, если функция живучести ниже допустимого предела ($j_m \le 0{,}8$; $k = 0{,}7$), то либо фиксируется P и уменьшаются нижний $t_н$ и верхний $t_в$ пределы времени восстановления работоспособности, либо при фиксированных $t_н$ и $t_в$ принимаются меры по уменьшению вероятности (повышается защищенность) поражения ОИ при нанесении КА. Требуемый ресурс оценивается и сравнивается с выгодой от получаемого коэффициента снижения страховой премии.

Для графика $t_н = 0{,}25$ сут и $t_в = 0{,}5$ сут значение $j_m \approx 0{,}68$ не удовлетворяет требованиям для получения снижающего коэффициента ($0{,}9 \ge j_m \ge 0{,}8$; $k = 0{,}7$). Последовательно уменьшая $t_н$ и $t_в$, осуществляя статистическое моделирование и отображая результаты графически, осуществляем поиск варианта, когда $j_m \approx 0{,}81$, т. е. незначительно превышает требуемое значение. Искомое решение – $t_н = 0{,}1$ сут (2,4 ч) и $t_в = 0{,}2$ сут (4,8 ч). Для достижения такого результата потребуется увеличение ресурса, выделяемого для поддержания защищенности ОИ и наращивания возможностей системы восстановления работоспособности ОИ.

Приведенная модель может быть использована для определения неблагоприятных моментов времени, когда функция живучести будет иметь локальные минимумы. Для исходных данных предыдущего примера, когда $t_н = 0{,}25$ сут (6 ч) и $t_в = 0{,}5$ сут (12 ч), получаем, что первый локальный минимум будет в окрестности точки $t_1 = 0{,}5$ от начала МКА, при $t_2 = 12$ ч $j_m \approx 0{,}81$, при $t_3 = 24$ ч $j_m \approx 0{,}8$. Знание этих моментов позволит лицу, принимающему решение (ЛПР), сосредоточить усилия на обеспечении живучести ОИ другими способами. Результаты моделирования для обозначенных выше исходных данных приведены на рис. 3.

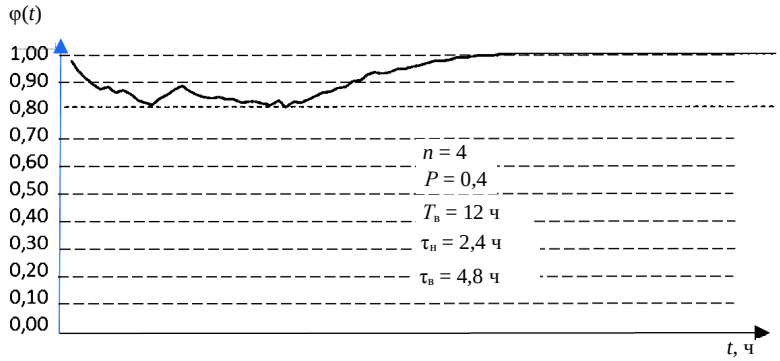


Рис. 3. График функции живучести $j(t)$ для плана поддержания непрерывности бизнеса, удовлетворяющая требованиям (усреднено 2 000 реализаций)

Fig. 3. Survivability features $j(t)$ for business continuity plan meeting the requirements (averaged 2, 000 implementations)

Также построенную модель можно использовать для проверки соответствия результатов аналитического и статистического моделирования функции живучести ОИ для различных планов поддержания непрерывности деловых процессов. Проверка может осуществляться с целью оценки: а) корректности выведенных аналитических выражений для функции живучести; б) точности результатов статистического моделирования. Если вероятность поражения объекта атаки неизвестна, то рекомендуется выбирать ее значение 0,5.

В результате внедрения вышерассмотренной статистической модели стало возможным моделирование альтернирующих процессов для законов распределения, отличных от экспоненциальных. Метод применим для моделирования при организации аудита ИБ.

Моделирование сценариев массированных компьютерных атак

Представляет практический интерес применение метода Монте-Карло для моделирования процессов функционирования ОИ в условиях МКА с учетом важности объекта КА в составе вычислительной сети (ВС), для чего в состав модели был введен блок задания различных сценариев реализации атак.

Вербальная постановка задачи:

Дано:

а) структура ($0 – N$) – полюсного ОИ, где N – количество элементов, представляющих конечные вершины, 0 – индекс управляющего элемента – вершина сети; от 1 до N – элементы, конечные вершины;

б) требования к коэффициенту готовности ОИ;

в) подмножество управляемых элементов, которые включены в технологическую цепочку (ха-

рактерную для периода атаки) и являются элементами ОИ.

Требуется: обеспечить обмен технологической информацией между ЛПР и объектами управления (конечные вершины ОИ).

Цель атакующего – нанести максимальный ущерб управляемости ОИ (минимизировать число конечных вершин ОИ, имеющих связи с ЛПР).

Постановка частной задачи:

Исходные данные:

а) n – число атак;

б) структура (1-N), 1 – полюс ЛПР, N – полюса управляемых объектов (УО);

в) пороговое число управляемых объектов $N_{тр}$, имеющих хотя бы одну связь с ЛПР, при котором обеспечивается управляемость АСУ ТП;

г) структура сети связи ОИ – $S_{ОИ} = (V, E)$, где:

– $V = \{v_i\}$ – множество узловых элементов ОИ, $v_i = 1$, если элемент находится в работоспособном состоянии, $v_i = 0$ в ином случае, $i = 0, 1, 2, \ldots, K$, K – число узловых элементов ВС, $i = 0$, индекс полюса ЛПР, $i = 1$ до K – индексы узловых элементов ОИ;

– $E = \{e_{ij}\}$ – множество линий связей между узловыми элементами V, $e_{ij} = 1$, если связь между i-м и j-м узлами предусмотрена, $e_{ij} = 0$, если связь между узлами не предусмотрена, $i = 1, 2, \ldots, K$-1, $j = 2, 3, \ldots, K$, K – число элементов множества V, включая управляющий элемент и N – управляемых элементов;

– $V^* = \{v^*\} \in V$ – подмножество управляемых объектов, которые находятся под управлением ЛПР.

Сценарии МКА:

1. Атакующему неизвестна принадлежность элементов вычислительной сети к ОИ.

2. Источнику КА неизвестна структура вычислительной сети ОИ – $S_{ОИ}$, но имеются сведения о принадлежности к ОИ.

3. Источнику КА известна $S_{ОИ}$, он способен оценить структурную важность элементов $S_{вч}$ и спланировать первую и последующие КА с учетом структурной важности элементов $S_{ОИ}$. Компьютерная атака планируется по критерию убывания w_i, где w_i – коэффициент структурной важности элемента, который рассчитывается согласно [18].

4. Источнику атаки известен результат предыдущей атаки, что позволяет ему скорректировать первоначальный сценарий атаки. Например, атака оказалась неуспешной, в результате цель атаки осталась непораженной (работоспособной), этот объект может быть снова включен в план атаки.

Ограничения:

1. Вероятность поражения элементов $S_{ОИ}$ – субъективная вероятность – задается посредством экспертных оценок [11–13] или находится с помощью статистической модели, приведенной выше.

2. Элементы $S_{ОИ}$ изменяют свое состояние (переходят из работоспособного состояния в пораженное и обратно) в момент времени t_i, где $i = 0 + \Delta t$, Δt – шаг дискретизации событий статистической модели.

3. Затраты на успешную атаку вершинного элемента (ЛПР) несоизмеримо велики по сравнению с успешными атаками на элементы $S_{ОИ}$.

4. Управляемые объекты – элементы множества V^* – равноценные.

С помощью лабораторного стенда [22]:

1. Вводятся исходные данные: а) о защищенности объекта атаки; б) о возможностях атакующего.

2. Обобщаются результаты реализаций моделирования.

3. Оценивается коэффициент оперативной готовности ОИ.

4. Осуществляется интерпретация полученного результата в условиях принятия решений при многих критериях [18] и в терминах, понятных ЛПР.

Таким образом, в статье описано решение актуальной научной задачи по оценке устойчивости объекта информатизации для условий МКА, имеющей практическое значение при страховании информационных рисков. Предлагаемый подход реализован как составная часть учебно-методического комплекса по подготовке аудиторской группы [22]. Исходные данные для планирования эксперимента с моделью приведены в [23].

Заключение

Получены частные выводы, которые представляют интерес для планирования дальнейших научных исследований в направлении совершенствования процессов выработки решений по обеспечению устойчивости функционирования ОИ в условиях целенаправленных агрессивных воздействий (МКА):

а) случайные атаки по рассматриваемой структуре вычислительной сети являются наименее эффективными;

б) зная структуру вычислительной сети, противник может наносить КА с учетом важности элементов. Данный способ реализации атаки является более эффективным по сравнению со случайными атаками;

в) зная структуру сети и имея план атаки с учетом структурной важности элементов, противник может нанести серьезный ущерб вычислительной сети меньшими затратами;

г) защита конфиденциальности структуры сети связи ОИ является обоснованной мерой обеспечения его живучести в условиях МКА.

Список источников

1. *Отчет* о сетевой безопасности и доступности в 2020 году. URL: https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf (дата обращения: 08.04.2021).

2. *2019 Data* Breach Investigations Report. URL: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (дата обращения: 08.04.2021).

3. *Макаренко С. И.* Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29.

4. *Лившиц И. И.* Современная практика аудита информационной безопасности // Управление качеством. 2011. № 7. С. 34–41.

5. *Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С. В.* Мониторинг и аудит информационной безопасности автоматизированных систем. М.: ИПУ им. В. А. Трапезникова РАН, 2009. 94 с.

6. *Марков А. С., Цирлов В. Л., Барабанов А. В.* Методы оценки несоответствия средств защиты информации / под ред. А. С. Маркова. М.: Радио и связь, 2012. 192 с.

7. *Воеводин В. А.* Методика аудита и мониторинга системы управления информационной безопасностью в части обеспечения защиты информации в вэб-приложениях // Современные исследования в области социально-общественных, экономических и технических наук: моногр. Н. Новгород: НОО «Профессиональная наука», 2021. С. 8–44.

8. *ГОСТ Р 51275–2006.* Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2018. 8 с.

9. *Воеводин В. А., Ковалев И. С., Фоломеев Л. А.* Страхование информационных рисков как инструмент управления защитой информации // Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2019: докл. Междунар. конф. (Москва, 29–31 мая 2019 г.). Сер.: Научн. конф., посвященные Дню Радио (вып. LXXV). М.: Изд-во Моск. НТО радиотехники, электроники и связи им. А. С. Попова, 2020. С. 152–155.

10. *ГОСТ Р 59516-2021.* Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности. М.: Стандартинформ, 2021. 20 с.

11. *Воеводин В. А., Маркин П. В., Маркина М. С., Буренок Д. С.* Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий // Системы управления, связи и безопасности. 2021. № 2. С. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129.

12. *Коробов В. Б.* Теория и практика экспертных методов: моногр. М.: ИНФРА-М, 2019. 282 с.

13. *Орлов А. И.* Организационно-экономическое моделирование: учеб.: в 3 ч. М.: Изд-во МГТУ им. Н. Э. Баумана, 2009. Ч. 2. Экспертные оценки. 2011. 486 с.

14. *Литвак Б. Г.* Экспертные оценки и принятие решений. М.: Патент, 1996. 271 с.

15. *Бешелев С. Д., Гурвич Ф. Г.* Математико-статистические методы экспертных оценок. М.: Статистика, 1980. 263 с.

16. *С-во* о гос. регистрации программы для ЭВМ 2020616093 РФ. Программа метода экспертных оценок / В. А. Воеводин, Д. С. Буренок; зарег. 22.05.2020; опубл. 09.06.2020.

17. *С-во* о гос. регистрации программ для ЭВМ № 2020667542 РФ. Программа метода анализа иерархий / В. А. Воеводин, Д. С. Буренок, П. В. Маркин, М. С. Маркина; опубл. 24.12.2020.

18. *Хохлачев Е. Н.* Организация и технологии выработки решений при управлении системой и войсками связи. М.: ВА РВСН, 2009. Ч. 2. Выработка решений при восстановлении сетей связи. 241 с.

19. *Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д.* Математические методы в теории надежности. М.: Наука, 1965. 524 с.

20. *С-во* о гос. регистрации программы для ЭВМ № 2021663763 РФ. Программа оценки минимума функции живучести объекта информатизации / В. А. Воеводин; опубл. 23.08.2021.

21. *С-во* о гос. регистрации программ для ЭВМ № 2020616191 РФ. Компьютерная программа оценки готовности АСУ ТП в условиях компьютерных атак / В. А Воеводин, Д. С. Ганенков, Н. В. Кучин; опубл. 11.06.2020.

22. *Воеводин В. А., Настинов Э. О.* Об учебно-методическом комплексе подготовки к аудиту информационной безопасности // Информационные технологии в государственном управлении. Цифровая трансформация и человеческий капитал: сб. науч. тр. XVIII Науч.-практ. конф. (25 апреля 2019 г.) М.: Проспект, 2019. С. 216–222.

23. *С-во* о гос. регистрации базы данных № 2021621344. База данных объективных свидетельств аудита информационной безопасности / В. А. Воеводин, Д. С. Буренок; опубл. 22.06.2021.

References

1. *Otchet o setevoi bezopasnosti i dostupnosti v 2020 godu* [Report on Network security and Availability in 2020]. Avaliable at: https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf (accessed: 08.04.2021).

2. *2019 Data Breach Investigations Report*. Avaliable at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (accessed: 08.04.2021).

3. Makarenko S. I. Audit informatsionnoi bezopasnosti: osnovnye etapy, kontseptual'nye osnovy, klassifikatsiia meropriiatii [Information security audit: main stages, conceptual framework, classification of activities]. *Sistemy upravleniia, sviazi i bezopasnosti*, 2018, no. 1, pp. 1-29.

4. Livshits I. I. Sovremennaia praktika audita informatsionnoi bezopasnosti [Modern practice of information security audit]. *Upravlenie kachestvom*, 2011, no. 7, pp. 34-41.

5. Kul'ba V. V., Shelkov A. B., Gladkov Iu. M., Pavel'ev S. V. *Monitoring i audit informatsionnoi bezopasnosti avtomatizirovannykh sistem* [Monitoring and audit of information security of automated systems]. Moscow, IPU im. V. A. Trapeznikova RAN, 2009. 94 p.

6. Markov A. S., Tsirlov V. L., Barabanov A. V. *Metody otsenki nesootvetstviia sredstv zashchity informatsii* [Methods for assessing the inconsistency of information security tools]. Pod redaktsiei A. S. Markova. Moscow, Radio i sviaz' Publ., 2012. 192 p.

7. Voevodin V. A. Metodika audita i monitoringa sistemy upravleniia informatsionnoi bezopasnost'iu v chasti obespecheniia zashchity informatsii v veb-prilozheniiakh [Methods of auditing and monitoring information security management system in terms of ensuring protection of information in web applications]. *Sovremennye issledovaniia v oblasti sotsial'no-obshchestvennykh, ekonomicheskikh i tekhnicheskikh nauk: monografiia*. Nizhnii Novgorod, NOO «Professional'naia nauka», 2021. Pp. 8-44.

8. GOST R 51275–2006. *Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeistvuiushchie na informatsiiu. Obshchie polozheniia* [GOST R 51275–2006. Data protection. Informatization object. Factors affecting information. General provisions]. Moscow, Standartinform Publ., 2018. 8 p.

9. Voevodin V. A., Kovalev I. S., Folomeev L. A. Strakhovanie informatsionnykh riskov kak instrument upravleniia zashchitoi informatsii [Insurance of information risks as tool for managing information protection]. *Radioelektronnye ustroistva i sistemy dlia infokommunikatsionnykh tekhnologii – REUS-2019: doklady Mezhdunarodnoi konferentsii (Moskva, 29–31 maia 2019 g.). Seriia: Nauchnye konferentsii, posviashchennye Dniu Radio (vypusk LXXV)*. Moscow, Izd-vo Mosk. NTO radiotekhniki, elektroniki i sviazi im. A. S. Popova, 2020. Pp. 152-155.

10. GOST R 59516-2021. *Informatsionnye tekhnologii. Menedzhment informatsionnoi bezopasnosti. Pravila strakhovaniia riskov informatsionnoi bezopasnosti* [GOST R 59516-2021. Information Technology. Information security management. Information security risk insurance rules]. Moscow, Standartinform Publ., 2021. 20 p.

11. Voevodin V. A., Markin P. V., Markina M. S., Burenok D. S. Metodika razrabotki programmy audita informatsionnoi bezopasnosti s uchetom vesovykh koeffitsientov znachimosti svidetel'stv audita na osnove metoda analiza ierarkhii [Technique for developing an information security audit program taking into account the weight coefficients of the significance of audit evidence based on the hierarchy analysis method]. *Sistemy upravleniia, sviazi i bezopasnosti*, 2021, no. 2, pp. 96-129. DOI: 10.24412/2410-9916-2021-2-96-129.

12. Korobov V. B. *Teoriia i praktika ekspertnykh metodov: monografiia* [Theory and practice of expert methods: monograph]. Moscow, INFRA-M Publ., 2019. 282 p.

13. Orlov A. I. *Organizatsionno-ekonomicheskoe modelirovanie: uchebnik: v 3 chastiakh* [Organizational and economic modeling: textbook: in 3 parts]. Moscow, Izd-vo MGTU im. N. E. Baumana, 2009. Part 2. Ekspertnye otsenki. 2011. 486 p.

14. Litvak B. G. *Ekspertnye otsenki i priniatie reshenii* [Expert assessments and decision making]. Moscow, Patent Publ., 1996. 271 p.

15. Beshelev S. D., Gurvich F. G. *Matematiko-statisticheskie metody ekspertnykh otsenok* [Mathematical-statistical methods of expert assessments]. Moscow, Statistika Publ., 1980. 263 p.

16. Voevodin V. A., Burenok D. S. *Programma metoda ekspertnykh otsenok* [Program of expert assessments method]. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM 2020616093 RF; 09.06.2020.

17. Voevodin V. A., Burenok D. S., Markin P. V., Markina M. S. *Programma metoda analiza ierarkhii* [Hierarchy analysis method program]. Svidetel'stvo o gosudarstvennoi registratsii programm dlia EVM № 2020667542 RF; 24.12.2020.

18. Khokhlachev E. N. *Organizatsiia i tekhnologii vyrabotki reshenii pri upravlenii sistemoi i voiskami sviazi* [Organization and technologies for making decisions in management of system and signal troops]. Moscow, VA RVSN, 2009. Part 2. Vyrabotka reshenii pri vosstanovlenii setei sviazi. 241 p.

19. Gnedenko B. V., Beliaev Iu. K., Solov'ev A. D. *Matematicheskie metody v teorii nadezhnosti* [Mathematical methods in reliability theory]. Moscow, Nauka Publ., 1965. 524 p.

20. Voevodin V. A. *Programma otsenki minimuma funktsii zhivuchesti ob"ekta informatizatsii* [Program for estimating minimum function of survivability of informatization object]. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM № 2021663763 RF; 23.08.2021.

21. Voevodin V. A., Ganenkov D. S., Kuchin N. V. *Komp'iuternaia programma otsenki gotovnosti ASU TP v usloviiakh komp'iuternykh atak* [Computer program for assessing the readiness of industrial control systems under conditions of computer attacks]. Svidetel'stvo o gosudarstvennoi registratsii programm dlia EVM № 2020616191 RF; 11.06.2020.

22. Voevodin V. A., Nastinov E. O. Ob uchebno-metodicheskom komplekse podgotovki k auditu informatsionnoi bezopasnosti [On educational and methodological complex of preparation for audit of information security]. *Informatsionnye tekhnologii v gosudarstvennom upravlenii. Tsifrovaia transformatsiia i chelovecheskii kapital: sbornik nauchnykh trudov XVIII Nauchno-prakticheskoi konferentsii (25 aprelia 2019 g.)*. Moscow, Prospekt Publ., 2019. Pp. 216-222.

23. Voevodin V. A., Burenok D. S. *Baza dannykh ob"ektivnykh svidetel'stv audita informatsionnoi bezopasnosti* [Database of objective evidence of information security audit]. Svidetel'stvo o gosudarstvennoi registratsii bazy dannykh № 2021621344; 22.06.2021.

Статья поступила в редакцию 21.03.2022; одобрена после рецензирования 28.03.2022; принята к публикации 12.04.2022
The article is submitted 21.03.2022; approved after reviewing 28.03.2022; accepted for publication 12.04.2022

Информация об авторе / Information about the author

Владислав Александрович Воеводин – кандидат технических наук; доцент кафедры информационной безопасности; Национальный исследовательский университет «Московский институт электронной техники»; vva541@mail.ru

Vladislav A. Voevodin – Candidate of Technical Sciences; Assistant Professor of the Department of Information Security; National Research University of Electronic Technology; vva541@mail.ru