УДК 519.718
doi:10.31799/1684-8853-2022-3-31-44

Научные статьи
Articles

Оценивание эффективности процесса функционирования системы обеспечения информационной безопасности на основе теории стохастической индикации

А. М. Сухов[a], *канд. техн. наук, докторант, orcid.org/0000-0003-2233-811X, 19am87@mail.ru*
[a]*Краснодарское высшее военное училище им. генерала армии С. М. Штеменко, Красина ул., 4, Краснодар, 350065, РФ*

Введение: *постоянный рост деструктивных воздействий, направленных на критические информационные системы в условиях несовершенства методов и средств обнаружения и реагирования на компьютерные атаки, вызывает необходимость разработки научно-методического аппарата своевременного предупреждения систем обеспечения информационной безопасности о возможной реализации сценариев деструктивных воздействий. Одним из эффективных путей решения данной проблемы является использование методов теории стохастической индикации.* ***Цель:*** *разработка инструмента для оценивания эффективности процесса функционирования системы обеспечения информационной безопасности.* ***Результаты:*** *описаны детерминированная, случайная и неопределенная составляющие процесса функционирования системы обеспечения информационной безопасности. Построены константные и функциональные индикаторы, раскрыты их отличительные особенности. Построены стохастические супериндикаторы для решения задачи оценивания эффективности рассматриваемого процесса. На основе теории эффективности целенаправленных процессов и целеустремленных систем описаны особенности построения стохастических индикаторов различного ранга.* ***Практическая значимость:*** *благодаря разработанным стохастическим временным индикаторам оцениваются вероятностно-временные характеристики деструктивного воздействия с учетом интервалов и моментов времени процесса его реализации, что позволяет своевременно информировать систему о возможном выполнении сценария деструктивного воздействия на элементы критической информационной инфраструктуры.*

Ключевые слова *— система обеспечения информационной безопасности, атомарное событие информационной безопасности, деструктивное воздействие, эффективность, качество, теория стохастической индикации.*

Для цитирования: Сухов А. М. Оценивание эффективности процесса функционирования системы обеспечения информационной безопасности на основе теории стохастической индикации. *Информационно-управляющие системы*, 2022, № 3, с. 31–44. doi:10.31799/1684-8853-2022-3-31-44

For citation: Sukhov A. M. Evaluating the effectiveness of the information security system process based on the theory of stochastic indicators. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 31–44 (In Russian). doi:10.31799/1684-8853-2022-3-31-44

Введение

Проблемы оценивания эффективности информационных систем начинаются с неоднозначности исходных определений. В отечественной и зарубежной литературе [1–6] даны различные по своей сути определения эффективности. Так, Г. Б. Петуховым был введен показатель эффективности, рассматриваемый как вероятностная мера соответствия характеристик случайных эффектов целенаправленного процесса требуемым (директивно заданным) значениям этих характеристик [7].

Нередко эффективность функционирования систем оценивалась методами, тесно связанными с функционированием современного рынка [8–10]. Исследования операционной системы приведены в работах [11–14].

В отличие от зарубежных подходов, оценивание различных операционных свойств систем в рамках российской школы исследования реализуется количественно.

Под эффективностью будем понимать комплексное операционное свойство целенаправленного процесса применения системы, характеризующее его приспособленность к достижению цели проводимой операции [7, 15, 16]. К наиболее полной характеристике степени достижения цели операции, которую проводит система обеспечения информационной безопасности (СОИБ), относится показатель пригодности (на основе семейства временных индикаторов). Им может служить вероятность $P_{\text{д.ц}} = P\left(\tau_{\text{н}} < \hat{\tau} \le \tau_{\text{д}}\right) = F_{\hat{\tau}}\left(\tau_{\text{д}}\right) - F_{\hat{\tau}}\left(\tau_{\text{н}}\right)$, где $\tau_{\text{н}}$ — минимально необходимые технологические затраты операционного времени для выполнения задачи с требуемым качеством; $\tau_{\text{д}}$ — директивное операционное время выполнения задачи.

При исследовании эффективности операции (целенаправленного процесса функционирования) наиболее типичной является ситуация, когда основные характеристики системы и параметры условий ее применения подвержены воздействию случайных факторов. Высокая стоимость СОИБ, сложность и масштабность решаемых задач, а также большие потери из-за ошибок в процессе их производства и испытаний стимулируют исследования эффективности использования систем данного рода.

Понятие стохастического супериндикатора

Современный уровень зависимости общества от информационных технологий обусловливает появление новых типов деструктивных воздействий (ДВ) и построения надежной СОИБ единого информационного пространства (ЕИП) [17–19]. В работе под деструктивным воздействием понимается целенаправленное, скоординированное воздействие либо на информационный ресурс, либо на информационную систему или на средства получения, передачи, обработки, хранения и воспроизведения информации в ее составе с целью вызвать заданные структурные и (или) функциональные изменения. Большинство, а в ряде случаев все средства защиты информации (СЗИ), входящие в состав СОИБ ЕИП, используют в своем арсенале датчики обнаружения (ДО), распознавания (ДР) и предупреждения (ДП) [20, 21]. Для краткости излагаемого материала ограничимся приведенными типами датчиков, которые в зависимости от реализуемой ими функции направлены на обнаружение $f_{\text{о}}(r)$, распознавание $f_{\text{р}}(r)$ и предупреждение $f_{\text{п}}(r)$ ДВ (рис. 1) и построены на основе индикаторов обнаружения $I_{\text{о}}$, распознавания $I_{\text{р}}$ и предупреждения $I_{\text{п}}$. Допустим, что СОИБ проводит операцию распознавания ДВ типа «Отказ в обслуживании» в ЕИП, тогда ДВ необходимо представить в виде множества J с различными r-ми типами возможных ДВ, направленных на снижение требуемого уровня защищенности ЕИП, где $J=\left\{j_1^r,\ j_2^r,\ j_3^r,\ \ldots,\ j_m^r\right\},\ r=\overline{1(1)R},\ m=\overline{1(1)M}$.

Отсюда следует, что СОИБ распознает r-й тип из множества J ДВ, если индикатор $I_{\text{р}}$ распознавания, по значению которого датчик просигнализирует СОИБ, примет вид

$$I_J=I_{\text{р}}(r)\overset{\text{def}}{=}\begin{cases}1,\ r\in J;\\ 0,\ r\notin J.\end{cases} \tag{1}$$

Множеству J r-х типов ДВ соответствует его индикатор, и, наоборот, каждая функция, принимающая лишь одно из двух значений {0, 1}, может интерпретироваться как индикатор некоторого множества и может быть задана линейным выражением

$$I_J(r)\times f(r)=\begin{cases}f(r),\ r\in J;\\ 0,\ r\notin J.\end{cases} \tag{2}$$

Пусть теперь D — пересечение, а B — объединение двух подмножеств j_1^r и j_2^r множества J r-х типов ДВ, т. е. $D=j_1^r\cap j_2^r$, $B=j_1^r\cup j_2^r$. Очевидно, что тогда

$$I_D=\inf\left\{I_{j_1^r},\ I_{j_2^r}\right\}=\min\left\{I_{j_1^r},\ I_{j_2^r}\right\}; \tag{3}$$

$$I_B=\sup\left\{I_{j_1^r},\ I_{j_2^r}\right\}=\max\left\{I_{j_1^r},\ I_{j_2^r}\right\}, \tag{4}$$

т. е. значение индикатора I_D или I_B множества D или B равно соответственно наименьшему или наибольшему из значений индикаторов $I_{j_1^r}$ и $I_{j_2^r}$. Поэтому для обозначения наименьшего или наибольшего из значений двух функций $f(r)$ и $g(r)$ используем теоретико-множественные обозначения:

$$\inf\left\{f(r),\ g(r)\right\}\overset{\text{def}}{=}f\cap g(r); \tag{5}$$

$$\sup\left\{f(r),\ g(r)\right\}\overset{\text{def}}{=}f\cup g(r). \tag{6}$$

Любой воздействующий на ЕИП r-й тип ДВ протекает в течение определенного интервала $\tau_{\text{р}}$ времени его реализации. Для уточнения структуры r-го типа ДВ необходимо произвести декомпозицию j_m^r ДВ на атомарные события информационной безопасности (АСИБ) $C=\left\{c_1^r,\ c_2^r,\ c_3^r,\ \ldots,\ c_l^r\right\},\ l=\overline{1(1)L}$ и построить индикатор реализации j_m^r ДВ. Впоследствии уточним из C АСИБ реализованный сценарий

$$j_m^r=\left\{\text{АСИБ}_1,\ \text{АСИБ}_2,\ \text{АСИБ}_3,\ \ldots,\ \text{АСИБ}_l\right\}=\left\{c_1^r,\ c_2^r,\ c_3^r,\ \ldots,\ c_l^r\right\}$$

ДВ с учетом $\tau_{\text{р}}$, равного $\tau_{\text{р}}=\tau_1+\tau'_{(1,2)}+\tau_2+\tau'_{(2,3)}+\tau_3+\tau'_{(3,k+1)}+\ldots+\tau_{k+1}$, где $\tau_{\text{р}}$ осуществляется только на интервале $\left[t'_1,\ t''_{k_l}\right)$, что наглядно представлено на рис. 2.

Для описания индикатора $I_{j_2^r}$ процесса реализации сценария $j_2^r=\left(c_1^r,\ c_2^r\right)$ ДВ, представленного на рис. 3, будем использовать кусочно-единичные («селектирующие») функции:

– «селектор луча»

$$\Delta\left(j_2^r\right)\overset{\text{def}}{=}\begin{cases}1,\ j_m^r\ge 0\\ 0,\ j_m^r<0\end{cases}; \tag{7}$$

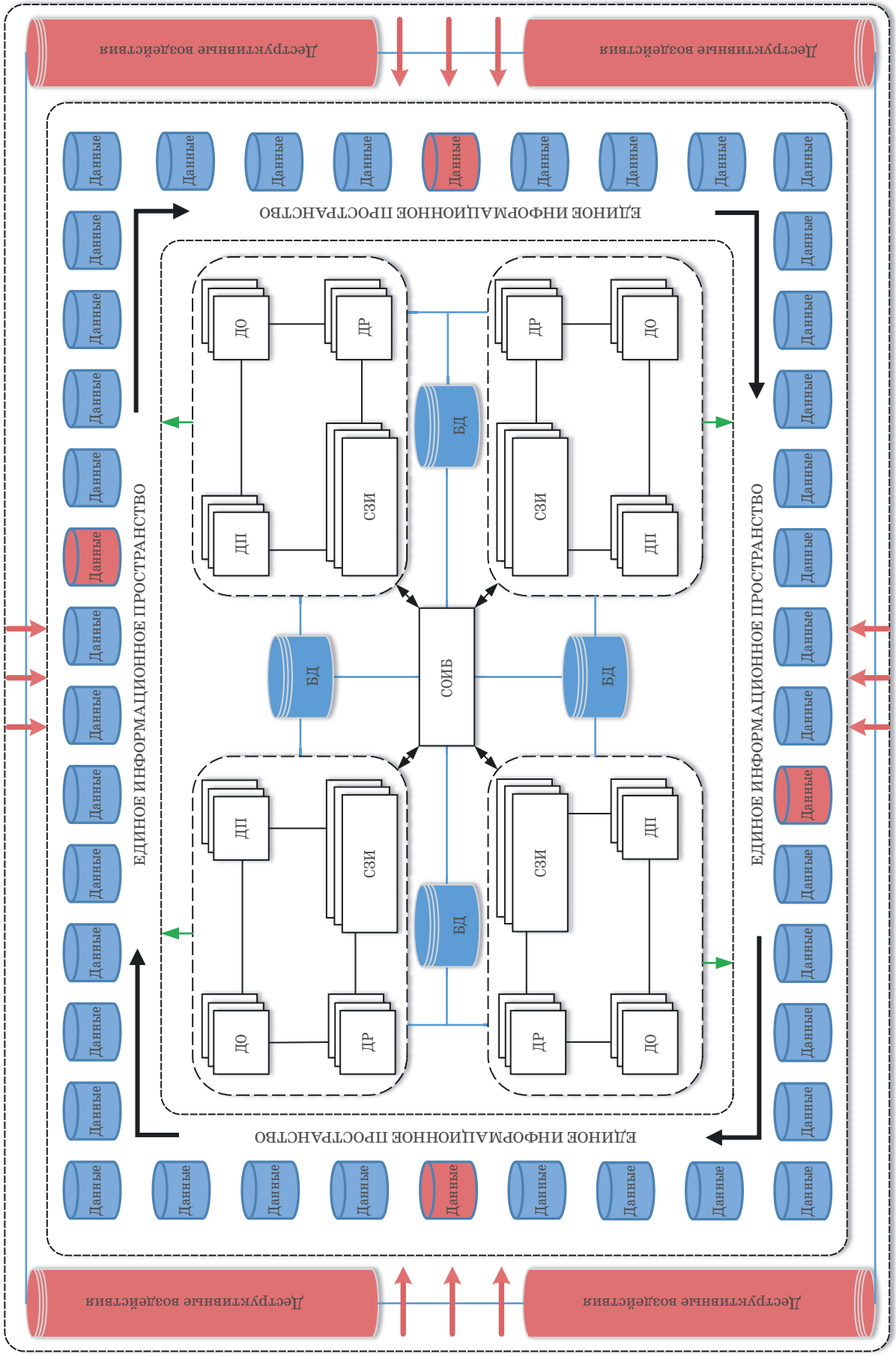
– «селектор интервала»

$$\prod\left(j_2^r;\ c_1^r,\ c_2^r\right)\overset{\text{def}}{=}\Delta\left(j_2^r-c_1^r\right)-\Delta\left(j_2^r-c_2^r\right)\triangleq\triangleq\Delta\left(j_2^r-c_1^r\right)\times\Delta\left(c_2^r-j_2^r\right); \tag{8}$$

– «селектор точки»

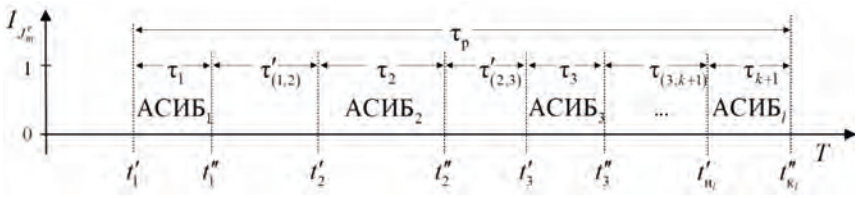
$$\varepsilon\left(j_2^r;\ a\right)\overset{\text{def}}{=}\Delta\left(j_2^r-a\right)\times\Delta\left(a-j_2^r\right). \tag{9}$$

Нетрудно видеть, что реализация C АСИБ, входящих в структуру сценария j_2^r ДВ, осущест-

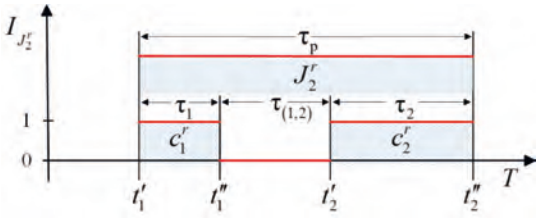


■ ■ *Рис. 1*. Структура процесса функционирования СОИБ в ЕИП

■ ■ *Fig. 1*. The structure of the process of functioning of the information security system in a single information space



■ ***Рис. 2.*** Индикатор реализации j_m^r ДВ
■ ***Fig. 2.*** Indicator of the implementation j_m^r of destructive impact



■ ***Рис. 3.*** Индикатор реализации $I_{j_2^r}$ ДВ
■ ***Fig. 3.*** Indicator of the implementation $I_{j_2^r}$ of destructive impact

вляется только на интервале $[t_1', t_2'']$, т. е. «селектор луча» («единичная функция Хевисайда») — суть индикатор полубесконечного интервала $[0, \infty)$:

$$\Delta\left(j_2^r\right) = I_J\left(j_2^r\right). \tag{10}$$

По аналогии с (10)

$$I'\left(j_2^r; c_1^r, c_2^r\right) = I_D\left(j_2^r\right), C = c_1^r \cap c_2^r,$$
$$c_1^r = [t_1', t_1''], c_2^r = [t_2', t_2''], \tag{11}$$

т. е. «селектор интервала» («единичный прямоугольный импульс») — индикатор интервала $[t_1', t_2'']$.

Таким образом, «селектор точки» («функция эквивалентности») — индикатор одноточечного множества $\{a\}$, который запишем в виде

$$\varepsilon\left(j_2^r; a\right) = I_{\{a\}}\left(j_2^r\right), \{a\} = a. \tag{12}$$

Если воспользоваться обозначением (5), то

$$\prod\left(j_2^r; c_1^r, c_2^r\right) = f \cap g\left(j_2^r\right), \tag{13}$$

где $f\left(j_2^r\right) = \Delta\left(j_2^r - c_1^r\right)$; $g\left(j_2^r\right) = \Delta\left(c_2^r - j_2^r\right)$.

И, соответственно:

$$\varepsilon\left(j_2^r; a\right) = f\left(j_2^r\right) \cap g\left(j_2^r\right), \tag{14}$$

где $f\left(j_2^r\right) = \Delta\left(j_2^r - c_1^r\right)$; $g\left(j_2^r\right) = \Delta\left(c_2^r - j_2^r\right)$.

Установлено, что кусочно-единичные («селектирующие») функции являются одним из немногих инструментов, позволяющих с высокой степенью детализации строить индикаторы $I_{j_2^r}$, показывающие множество $J = \left\{j_1^r, j_2^r, j_3^r, \ldots, j_m^r\right\}$ реализующихся сценариев ДВ r-х типов с учетом как самих интервалов времени $[t', t_k'']$ реализации j_m^r сценариев ДВ r-х типов, так и интервалов времени $[t_1', t_1'']$, $[t_2', t_2'']$, …, $\left[t_{k_l}', t_{k_{l+1}}''\right)$ реализации множества $C = \left\{c_1^r, c_2^r, c_3^r, \ldots, c_l^r\right\}$ АСИБ.

В современных условиях функционирования СОИБ наибольший для исследователей интерес представляют сценарии j_m^r ДВ r-х типов с вероятностной структурой. Предположим, что ДВ состоит из $\hat{C}$ АСИБ, $\hat{C} \subseteq X$ является случайным, так как заранее неизвестна структура ДВ (где X — универсальное множество, H — множество логических возможностей по обнаружению, распознаванию и предупреждению деструктивных возможностей злоумышленника, C — множество АСИБ). Введем допущение, что число АСИБ, составляющих сценарий j_m^r ДВ, является случайным. Временной интервал, на котором реализуются все АСИБ, входящие в состав сценария j_m^r ДВ, примем равным 1, достоверное событие (обнаружение реализации сценария j_m^r ДВ в ЕИП СОИБ) примем равным 1. Тогда индикатор обнаружения всего множества C АСИБ, входящих в состав сценария j_m^r ДВ, $I_{\hat{J}}$ будет представлять собой случайную величину $\hat{\omega}_J$ со следующими свойствами:

$$I_{\hat{J}} \overset{\text{def}}{=} \hat{\omega}_j = \begin{cases} 1, \text{ если } J \text{ произойдет;} \\ 0, \text{если } J \text{ не произойдет} \\ \left(\text{произойдет} \neg J\right). \end{cases} \tag{15}$$

В отличие от индикаторов $I_{\hat{J}}$ множеств сценариев j_m^r ДВ r-го типа, индикаторы $\hat{\omega}_J$ обнаружения на неопределенном интервале $\left(\hat{t}_{k_l}', \hat{t}_{k_{l+1}}''\right)$ времени их реализации носят случайный характер и называются стохастическими. В работе [7] авторы оперируют не случайными событиями, а предлагают переходить к случайным величинам, для которых в теории вероятностей разработан более гибкий и универсальный математический

аппарат. Таким образом, плотность распределения $\varphi_{\hat{\omega}_J}(\omega)$ и функция распределения $F_{\hat{\omega}_J}(\omega)$ стохастического индикатора $\hat{\omega}_J$ обнаружения сценариев j_m^r ДВ будут описываться следующими выражениями:

$$\varphi_{\hat{\omega}_J}(\omega) = q\delta(\omega) + p\delta(\omega - 1); \quad (16)$$

$$F_{\hat{\omega}_J}(\omega) = q\Delta(\omega) + p\Delta(\omega - 1), \quad (17)$$

где $p = P(\hat{J})$; $q = 1 - p = P(\neg \hat{J})$.

В свете вышеизложенного и с учетом (16), (17) из соотношения (15) следует

$$P(\hat{J}) = p = P(\hat{\omega}_J = 1) = M[\hat{\omega}_J] = \overline{\omega}_J. \quad (18)$$

Раскроем равенство (18), для чего воспользуемся содержательной трактовкой понятия случайного события $\hat{J}$. Допустим, что СОИБ выполняет функцию $f_o(r)$ обнаружения возможно реализующихся сценариев $\hat{J}$ ДВ, тогда под целенаправленным процессом ее функционирования стоит рассматривать операцию обнаружения признака C АСИБ, по которому СОИБ будет реализовывать функцию $f_p(r)$ распознавания сценария $\hat{j}_m^r$ ДВ r-го типа, тогда под $\hat{J}$ понимается исход операции обнаружения сценария $\hat{j}_m^r$ ДВ r-го типа, состоящей в реализации условий B', B'', где B' — условия функционирования СОИБ, а B'' — условия применения СОИБ, при которых СОИБ хочет обнаружить сценарии j_m^r ДВ r-го типа. Тогда случайное событие $\hat{J}$ есть не что иное, как исход операции обнаружения сценария j_m^r ДВ r-го типа, проходящей при воздействии на B', B'' не поддающихся учету случайных факторов, т. е. в условиях $\hat{B}'$, $\hat{B}''$ некоторой неопределенности, приводящей к тому, что обнаружение сценария j_m^r ДВ r-го типа происходит не при каждой реализации условий B', B''. Следовательно, связь между обнаружением признака C АСИБ, принадлежащего одному из сценариев j_m^r ДВ r-го типа, и предопределяющими $\hat{B}'$, $\hat{B}''$ условиями носит случайный характер. Количественное оценивание проводимой СОИБ в ЕИП операции обнаружения сценария j_m^r ДВ r-го типа будем выполнять при помощи вероятности $P(\hat{J})$ обнаружения случайного $\hat{C}$ АСИБ, которая характеризует степень объективной возможности обнаружения сценария $\hat{j}_m^r$ ДВ r-го типа в условиях $\hat{B}'$, $\hat{B}''$.

Проведем аналогию высказывания относительно обнаружения сценария j_m^r ДВ r-го типа и условий B' функционирования СОИБ и B'' применения, в которой оно истинно. Действительно, при решении конкретных прикладных задач информационной безопасности описание любого из исследуемых событий дается в форме некоторого высказывания (предположения, гипотезы). Истинность высказывания обнаружения сценария j_m^r ДВ r-го типа адекватна достоверности его обнаружения СОИБ в процессе выполнения функции $f_o(r)$. Аналогом множества $J = \{j_1^r, j_2^r, j_3^r, \ldots, j_m^r\}$ ДВ r-го типа, нарушающих установленную администратором информационной безопасности политику, является множество логических возможностей $H = \{h_1^r, h_2^r, h_3^r, \ldots, h_w^r\}$ (при которых высказывание J истинно), называемое множеством истинности высказывания J. Основываясь на описанном выше, получаем возможность вести содержательное описание функции $f_o(r)$ обнаружения вероятно реализующихся сценариев $\hat{J}$ ДВ СОИБ в терминах алгебры высказываний, что применительно к возложенным функциям по обнаружению $f_o(r)$, распознаванию $f_p(r)$ и предупреждению $f_п(r)$ ДВ в ЕИП на СОИБ обладает большей наглядностью, чем описание на языке алгебры событий, т. е.

$$I_J(r) = \begin{cases} 1, & r \in J,\ J \subseteq X; \\ 0, & r \notin J,\ J \subseteq X. \end{cases} \quad (19)$$

Необходимо отметить, что истинность и ложность высказывания по обнаружению сценария j_m^r ДВ r-го типа эквивалентны соответственно достоверности и невозможности обнаружения сценария j_m^r ДВ r-го типа, а стохастичность ситуации $\hat{B}'$, $\hat{B}''$, в которой высказывание истинно, эквивалентна неопределенности условий $\hat{B}'$, $\hat{B}''$, определяющих случайный эксперимент (единичную операцию обнаружения сценария j_m^r ДВ r-го типа при неопределенных условиях B' функционирования СОИБ и B'' применения соответственно). При такой трактовке очевидно, что каждая из алгебр (высказываний и событий) является булевой и изоморфна алгебре их индикаторов $I_J(r)$. Следовательно, эти алгебры изоморфны между собой и неопределенная ситуация на языке любой из них адекватна и применима для построения индикаторов обнаружения I_o, распознавания I_p и предупреждения $I_п$, на основе которых построены ДО, ДР и ДП (см. рис. 1).

Количественные характеристики неопределенности стохастической ситуации при исследовании процессов функционирования СОИБ

В целях определения количественных характеристик необходимо описать детерминированную, случайную и неопределенную составляющие процесса функционирования СОИБ.

Детерминированными подразумеваем процессы, вызванные действием полностью известных

условий B', B''. Такие процессы практически не встречаются в современных условиях (только лишь на этапах проектирования СОИБ, в моделях, не учитывающих J_m ДВ злоумышленника).

Случайные процессы (ошибки операторов, запуск вредоносного программного обеспечения, превышенное количество обращений легитимных пользователей и др.) возникают при воздействии не поддающихся учету $\hat{B}''$ условий применения, на известные причины B' условий функционирования СОИБ, делающих причины $\hat{B} = B' \cup \hat{B}''$, и основные свойства процесса случайными.

В связи с недостаточностью (не в полной мере учтены возможности возмущающей среды) или отсутствием наблюдений (число опытов таких систем на практике невелико, так как реализуемые злоумышленниками J ДВ в современных условиях носят уникальный, единичный характер), необходимых для определения вероятностных свойств исследуемого процесса обнаружения сценариев j_m^r ДВ r-го типа, неопределенным становится и сам процесс обнаружения сценариев $\hat{j}_m^r$ ДВ r-го типа СОИБ в условиях $\hat{B}'$, $\hat{B}''$.

Не вдаваясь в сравнительный анализ понятий «случайность» и «неопределенность», а также связанных с ними понятий «объективная» и «субъективная» вероятности, отметим, что в принципе различия между ними чисто условны. С одной стороны, при наблюдении реальных процессов функционирования СОИБ их случайность и неопределенность проявляются одинаково — как невозможность точного прогнозирования момента $t_{\text{обн}}$ обнаружения C АСИБ, входящих в состав сценария j_m^r ДВ r-го типа, на интервале $(t_{\text{н}}, t_{\text{к}})$ времени; с другой стороны, «объективные» вероятностные характеристики случайных процессов не могут быть полностью свободными от «субъективных» взглядов их исследователей. Даже задаваемые экспертами «субъективные» вероятности в значительной мере являются «объективными», поскольку основаны на опыте изучения экспертами случаев применения СОИБ.

Таким образом, степень случайности вышеупомянутого высказывания охарактеризуем его вероятностью $P\left(\hat{J}\right) = p$. В случае обнаружения сценария j_m^r ДВ r-го типа СОИБ высказывание J окажется истинным, и его вероятность станет равной 1, а если СОИБ не справится с обнаружением сценария j_m^r ДВ r-го типа, высказывание J окажется ложным, и его вероятность, соответственно, будет равна 0. Поскольку априори неизвестно, истинным или ложным окажется высказывание $\hat{J}$, следовательно, неизвестно, какое из значений (1 или 0) примет его вероятность, которая, таким образом, является случайной величиной, подчиненной закону распределения Бернулли с параметром p. Именно так и распределен стохастический индикатор $\hat{\omega}_J$ обнаружения сценария j_m^r ДВ r-го типа на неопределенном интервале $\left(\hat{t}'_{k_l}, \hat{t}''_{k_{l+1}}\right)$ времени его реализации [см. (16), (17)], и, следовательно, он приобретает смысл условной вероятности высказывания $\hat{J}$ относительно ситуации B. В этом случае неопределенность ситуации $\hat{B}$ характеризуется набором {0, 1} возможных значений стохастического индикатора $\hat{\omega}_J$, а случайность высказывания $\hat{J}$ характеризуется его вероятностью p.

Формализация стохастической ситуации

Количественные характеристики при исследовании процессов функционирования СОИБ относительно ситуации B в значительной мере носят качественный характер, затрудняющий применение математических методов исследования. Для получения возможности количественного анализа таких ситуаций необходима их формализация, т. е. построение адекватных им математических моделей.

Предположим, что СОИБ производит наблюдение за реализацией сценария j_m^r ДВ r-го типа, который состоит из C АСИБ, где $C = \left\{c_1^r, c_2^r\right\}$. Интервал времени реализации сценария j_m^r ДВ r-го типа обозначим $\tau_{\text{р.с}}$. С учетом $C = \left\{c_1^r, c_2^r\right\}$, $\tau_{\text{р.с}} = \tau_1 + \tau_{\text{о}} + \tau_2$, где $\tau_1 = \left\langle t'_1, t''_1 \right\rangle$, а $\tau_2 = \left\langle t'_2, t''_2 \right\rangle$. Временной интервал между реализацией АСИБ обозначим $\tau_{\text{о}}$: $\tau_{\text{о}} = \left\langle t''_1, t'_2 \right\rangle$. Иллюстрирует сказанное рис. 4.

С учетом вышеизложенного пусть:

U — действительная прямая;

$U^2 \overset{\text{def}}{=} U \times U$ — действительная плоскость;

c_1^r, c_2^r — константы;

τ_1, τ_2 — переменные;

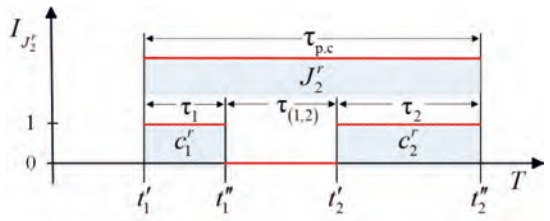
$<$, $>$, $\le$, $\ge$ — отношения порядка.

Тогда:

$c_1^r < c_2^r$, $c_1^r > c_2^r$, $c_1^r \le c_2^r$, $c_1^r \ge c_2^r$ — высказывания;

$\tau_2 < c_1^r$, $\tau_2 > c_1^r$, $\tau_2 \le c_2^r$, $\tau_2 \ge c_2^r$ — одноместные предикаты;

$\tau_2 < \tau_1$, $\tau_2 > \tau_1$, $\tau_2 \le \tau_1$, $\tau_2 \ge \tau_1$ — двухместные предикаты.



■ ***Рис. 4.*** Индикатор I_J сценария j_m^r ДВ r-го типа

■ ***Fig. 4.*** The indicator I_J of the j_m^r scenario is of destructive impact of the r-th type

Константы c_1^r, c_2^r фиксируют ситуацию реализации C АСИБ сценария j_m^r ДВ r-го типа на интервале $\langle t_1', t_2'' \rangle$ (см. рис. 4), в которой высказывание $c_1^r < c_2^r$ либо истинно (если $c_1^r < c_2^r$), либо ложно (если $c_1^r \geq c_2^r$). Практически всегда переменная $\hat{\tau}_2$ является случайной величиной, тогда для определения вероятности высказывания $\left(\hat{\tau}_2 < c_1^r\right)$ достаточно знать закон распределения $F_{\hat{\tau}_2}(\tau_2)$ случайной величины $\hat{\tau}_2$:

$$p = P\left(\hat{J}\right) = P\left(\hat{\tau}_2 < c_1^r\right) = \int_{-\infty}^{a} \mathrm{d}F_{\hat{\tau}_2}(\tau_2) = F_{\hat{\tau}_2}\left(c_1^r\right). \quad (20)$$

Когда $I_J(\hat{\tau}_2) = \hat{\omega}_J$ является стохастическим индикатором множества $J = \left(-\infty, c_1^r\right)$, то из выражений (18), (20) следует, что $P(\hat{\omega}_J = 1) = F_{\hat{\tau}_2}\left(c_1^r\right)$, и выражения (16), (17) примут вид

$$\varphi_{\hat{\omega}_J}(\omega) = R_{\hat{\tau}_2}\left(c_1^r\right) \times \delta(\omega) + F_{\hat{\tau}_2}\left(c_1^r\right) \times \delta(\omega - 1); \quad (21)$$

$$F_{\hat{\omega}_J}(\omega) = R_{\hat{\tau}_2}\left(c_1^r\right) \times \Delta(\omega) + F_{\hat{\tau}_2}\left(c_1^r\right) \times \Delta(\omega - 1). \quad (22)$$

Найдем числовые характеристики индикатора $\hat{\omega}_J$, который в дальнейшем будем называть константным. Начальный момент 1-го порядка распределения индикатора $\hat{\omega}_J$ определяется соотношением

$$v_k\left[\hat{\omega}_J\right] \overset{\text{def}}{=} M\left[\hat{\omega}_J^k\right] = \overline{\omega_J^k} = \int_{-\infty}^{\infty} \omega^k \mathrm{d}F_{\hat{\omega}_J}(\omega) = F_{\hat{\tau}_2}\left(c_1^r\right), \left[k = 1(1)K\right], \quad (23)$$

и, следовательно:

$$M_{\hat{\omega}_J} = \overline{\omega_J^1} = F_{\hat{\tau}_2}\left(c_1^r\right); \quad (24)$$

$$D_{\hat{\omega}_J} = \overline{\breve{\omega}_J^2} = \overline{\omega_J^2} - \overline{\omega}_J^2 = F_{\hat{\tau}_2}\left(c_1^r\right) - F_{\hat{\tau}_2}^2\left(c_1^r\right) = F_{\hat{\tau}_2}\left(c_1^r\right) \times R_{\hat{\tau}_2}\left(c_1^r\right). \quad (25)$$

Таким образом, как видно из равенства (24), вероятность случайного события $\hat{J}$ равна математическому ожиданию его индикатора $\hat{\omega}_J$.

Поскольку возможными значениями стохастического индикатора служат возможные степени достоверности случайного события $\hat{J}$, т. е. степени истинности неопределенного высказывания $\hat{\tau}_2 < c_1^r$, являющиеся значениями его апостериорной вероятности, то в рассматриваемом случае дисперсия $D_{\hat{\omega}_J}$ характеризует степень неопределенности предиката $\left(\hat{\tau}_2 < c_1^r\right) \simeq (\hat{\omega}_J = 1)$. При этом, как нетрудно понять, максимальная неопределенность будет иметь место при $c_1^r = \mathrm{Me}_{\hat{\tau}_2}$.

Рассмотрим неопределенный предикат $\hat{\tau}_2 < \tau_1$ и $\hat{\tau}_2 < \hat{\tau}_1$.

1. Переменная $\hat{\tau}_2$ случайна, тогда

$$p = p(\tau_1) = P\left(\hat{J}_{\tau_1}\right) = P(\hat{\tau}_2 < \tau_1) = \int_{-\infty}^{\tau_1} \mathrm{d}F_{\hat{\tau}_2}(\tau_2) = F_{\hat{\tau}_2}(\tau_1) = P\left[\hat{\omega}_J(\tau_1) = 1\right], \quad (26)$$

где $\hat{\omega}_J(\tau_1)$ — стохастический индикатор множества $J_{\tau_1} = (-\infty, \tau_1)$.

Из выражения (26) видно, что в данном случае $\hat{\omega}_{J_{\tau_1}} = \hat{\omega}_J(\tau_1) = \Delta(\tau_1 - \hat{\tau}_2)$ (рис. 5), т. е. формально индикатор случайного события $\hat{J}_{\tau_1}$ представляет собой случайную функцию, законы распределения которой имеют следующие выражения:

$$\varphi_{\hat{\omega}_{J_{\tau_1}}}(\omega;\, \tau_1) = R_{\hat{\tau}_2}(\tau_1) \times \delta(\omega) + F_{\hat{\tau}_2}(\tau_1) \times \delta(\omega - 1); \quad (27)$$

$$F_{\hat{\omega}_{J_{\tau_1}}}(\omega;\, \tau_1) = R_{\hat{\tau}_2}(\tau_1) \times \Delta(\omega) + F_{\hat{\tau}_2}(\tau_1) \times \Delta(\omega - 1). \quad (28)$$

Стохастический индикатор $\hat{\omega}_A(\tau_1)$ называется функциональным [7] с характеристиками

$$M\left[\hat{\omega}_J^k(\tau_1)\right] = \overline{\omega_J^k}(\tau_1) = \int_{-\infty}^{\infty} \omega^k \mathrm{d}F_{\hat{\omega}_{J_{\tau_1}}}(\omega;\, \tau_1) = F_{\hat{\tau}_2}(\tau_1); \quad (29)$$

$$M\left[\hat{\omega}_J(\tau_1)\right] = \overline{\omega}_J(\tau_1) = F_{\hat{\tau}_2}(\tau_1); \quad (30)$$

$$D\left[\hat{\omega}_J(\tau_1)\right] = \overline{\breve{\omega}_J^2} = \overline{\omega_J^2}(\tau_1) - \overline{\omega}_J^2(\tau_1) = F_{\hat{\tau}_2}(\tau_1) R_{\hat{\tau}_2}(\tau_1). \quad (31)$$

2. Переменная $\hat{\tau}_1$ также случайна, тогда предикат $\hat{\tau}_2 < \hat{\tau}_1$ становится дважды неопределенным, и вероятность случайного события $\hat{J}_{\hat{\tau}_1}$, при известной плотности распределения $\varphi_{\hat{\tau}_1, \hat{\tau}_2}(\tau_1, \tau_2)$, может быть представлена в виде

$$P\left(\hat{J}_{\hat{\tau}_1}\right) = P(\hat{\tau}_2 < \hat{\tau}_1) = P\left[\hat{\tau}_1, \hat{\tau}_2 \in (H)\right] = \iint_{(H)} \varphi_{\hat{\tau}_1, \hat{\tau}_2}(\tau_1, \tau_2) \mathrm{d}\tau_1 \, \mathrm{d}\tau_2, \quad (32)$$

где $(H) \cong \{\langle \tau_1, \tau_2 \rangle : \tau_2 < \tau_1\}$;

■ ***Рис. 5.*** Индикатор случайного события
■ ***Fig. 5.*** Indicator of a random event

$$P\left(\hat{J}_{\hat{\tau}_1}\right)=P\left(\hat{\tau}_2<\hat{\tau}_1\right)=P\left(\hat{u}<0\right)=\int\limits_{-\infty}^{0}\varphi_{\hat{u}}(u)\mathrm{d}u, \quad (33)$$

где $\hat{u}=\hat{\tau}_2-\hat{\tau}_1$;

$$P\left(\hat{J}_{\hat{\tau}_1}\right)=P\left(\hat{\tau}_2<\hat{\tau}_1\right)=P\left(\hat{\vartheta}\geq 0\right)=\int\limits_{0}^{\infty}\varphi_{\hat{\vartheta}}(\vartheta)\mathrm{d}\vartheta, \quad (34)$$

где $\hat{\vartheta}=\hat{\tau}_1-\hat{\tau}_2$.

При вышеприведенном определении вероятности случайного события $\hat{J}_{\hat{\tau}_1}$ (32), (33) теряется некоторый объем информации о реализации C АСИБ сценария J_m^r ДВ r-го типа на интервале $\left\langle t_1', t_2''\right\rangle$ (см. рис. 4). Для исследования реализации C АСИБ сценария J_m^r ДВ r-го типа на интервале $\left\langle t_1', t_2''\right\rangle$ с учетом сохранения информации преобразуем выражение (32):

$$\iint\limits_{(H)}\varphi_{\langle\hat{\tau}_1,\hat{\tau}_2\rangle}(\tau_1,\tau_2)\mathrm{d}\tau_1\mathrm{d}\tau_2=$$

$$=\iint\limits_{\tau_2<\tau_1}\varphi_{\langle\hat{\tau}_1,\hat{\tau}_2\rangle}(\tau_1,\tau_2)\mathrm{d}\tau_1\,\mathrm{d}\tau_2=$$

$$=\int\limits_{-\infty}^{\infty}\varphi_{\hat{\tau}_2}(\tau_2)\left[\int\limits_{\tau_1}^{\infty}\varphi_{\hat{\tau}_2/\hat{\tau}_1}(\tau_1;\tau_2)\mathrm{d}\tau_1\right]\mathrm{d}\tau_2=$$

$$=\int\limits_{-\infty}^{\infty}F_{\hat{\tau}_2/\hat{\tau}_1}(\tau_1;\tau_1)\mathrm{d}F_{\hat{\tau}_1}(\tau_1); \quad (35)$$

$$\iint\limits_{(H)}\varphi_{\langle\hat{\tau}_1,\hat{\tau}_2\rangle}(\tau_1,\tau_2)\mathrm{d}\tau_1\mathrm{d}\tau_2=$$

$$=\iint\limits_{\tau_2<\tau_1}\varphi_{\langle\hat{\tau}_1,\hat{\tau}_2\rangle}(\tau_1,\tau_2)\mathrm{d}\tau_1\mathrm{d}\tau_2=$$

$$=\int\limits_{-\infty}^{\infty}\varphi_{\hat{\tau}_2}(\tau_2)\left[\int\limits_{\tau_2}^{\infty}\varphi_{\hat{\tau}_2/\hat{\tau}_1}(\tau_1;\tau_2)\mathrm{d}\tau_1\right]\mathrm{d}\tau_2=$$

$$=\int\limits_{-\infty}^{\infty}R_{\hat{\tau}_2/\hat{\tau}_1}(\tau_2;\tau_2)\mathrm{d}F_{\hat{\tau}_2}(\tau_2). \quad (36)$$

В соотношениях (35) и (36) для определения искомой вероятности $p=P\left(\hat{\tau}_2<\hat{\tau}_1\right)$ описаны два пути, которые приводят к одному и тому же результату, но обеспечивают различную его надежность [7].

Наиболее распространенным с практической точки зрения является ситуация, когда случайные величины $\hat{\tau}_1$ и $\hat{\tau}_2$ взаимно независимы, тогда соотношения (35) и (36) примут вид

$$P\left(\hat{\tau}_2<\hat{\tau}_1\right)=\int\limits_{-\infty}^{\infty}F_{\hat{\tau}_2}(\tau_1)\mathrm{d}F_{\hat{\tau}_1}(\tau_1); \quad (37)$$

$$P\left(\hat{\tau}_1>\hat{\tau}_2\right)=\int\limits_{-\infty}^{\infty}R_{\hat{\tau}_1}(\tau_2)\mathrm{d}F_{\hat{\tau}_2}(\tau_2). \quad (38)$$

Введем следующие обозначения:

$$\hat{\omega}_1=\omega_1\left(\hat{\tau}_1\right)=F_{\hat{\tau}_2}(\tau_1); \quad (39)$$

$$\hat{\omega}_2=\omega_2\left(\hat{\tau}_2\right)=R_{\hat{\tau}_2}(\tau_2). \quad (40)$$

Случайные величины $\hat{\omega}_1$ и $\hat{\omega}_2$ называются стохастическими супериндикаторами, и с учетом введенных обозначений запишем

$$\left.\begin{aligned}P\left(\hat{\tau}_2<\hat{\tau}_1\right)=M\left[\hat{\omega}_1\right]=\bar{\omega}_1\\ P\left(\hat{\tau}_1>\hat{\tau}_2\right)=M\left[\hat{\omega}_2\right]=\bar{\omega}_2\end{aligned}\right\}\bar{\omega}_1=\bar{\omega}_2. \quad (41)$$

Соответственно:

$$P\left(\hat{\tau}_2<\hat{\tau}_1\right)=\bar{\omega}_1=\int\limits_{0}^{1}\omega\mathrm{d}F_{\hat{\omega}_1}(\omega)=\bar{\omega}_2=\int\limits_{0}^{1}\omega\mathrm{d}F_{\hat{\omega}_2}(\omega), \quad (42)$$

где $F_{\hat{\omega}_1}(\omega)$, $F_{\hat{\omega}_2}(\omega)$ — функции распределения супериндикаторов $\hat{\omega}_1$ и $\hat{\omega}_2$.

Основные свойства стохастических индикаторов

Константный $\left(\hat{\omega}_1\right)$ и функциональный $\left[\hat{\omega}_J(\tau_1)\right]$ индикаторы, определяющие соответственно апостериорные вероятности $\hat{J}$ и $\hat{J}_{\tau_1}$ обнаружения сценария J_m^r ДВ r-го типа, принимают лишь одно из двух значений (0 или 1), тогда как супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ могут принимать бесконечное множество значений из интервала (0, 1], т. е. являются случайными величинами более общего типа.

Таким образом, СОИБ будет обнаруживать любой сценарий J_m^r ДВ r-го типа с априорной вероятностью, равной математическому ожиданию условной вероятности $M\left[\hat{\omega}_1\right]$. Если достоверность событий $\hat{J}$ и $\hat{J}_{\tau_1}$ принимает лишь одно из двух значений: 0 или 1 с вероятностями q, p соответственно, — то достоверность события $\hat{J}_{\tau_1}$ распределена на интервале (0, 1] с плотностью $\varphi_{\hat{\omega}_1}(\omega)$ или $\varphi_{\hat{\omega}_2}(\omega)$.

Из равенств (34) и (40) следует, что $\hat{\omega}_J=P\left(\hat{\omega}_J=1\right)$; $\hat{\omega}_J(\tau_1)=P\left[\hat{\omega}_J(\tau_1)=1\right]$, но $\hat{\omega}_1\neq P\left(\hat{\omega}_1=1\right)$; $\hat{\omega}_2\neq P\left(\hat{\omega}_2=1\right)$. Различие является следствием того, что в последнем случае не только процесс обнаружения СОИБ в ЕИП сценария J_m^r ДВ r-го типа неопределенный, но и степень достоверности обнаружения $C=\left\{c_1^r, c_2^r\right\}$ АСИБ в составе сценария J_m^r ДВ r-го типа на интервале времени $\tau_{\text{р.с}}$ реализации сценария J_m^r ДВ r-го типа случайна и может принимать значения, отличные от 0 и 1.

Таким образом, супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ совмещают в себе свойства и функции $\omega\left(\hat{\tau}_1\right)$ случайного аргумента и случайной функции $\hat{\omega}(\tau_1)$ [см. (39), (40)].

Физический смысл заключается в следующем. Если интервал $\hat{\tau}_2$ времени обнаружения реализующегося c_1^r АСИБ случаен, то в предикате $\hat{\tau}_2 < c_1^r$ константа c_1^r определяет границу детерминированного множества $J = \left(-\infty, c_1^r\right)$, а в предикате $\hat{\tau}_2 < \tau_1$ переменная τ_1 определяет границу переменного множества $J = (-\infty, \tau_1)$, при попадании в которое случайной величины $\hat{\tau}_2$ индикаторы $\hat{\omega}_J$ и $\hat{\omega}_J(\tau_1)$ принимают значение 1. В предикате $\hat{\tau}_2 < \hat{\tau}_1$ переменная $\hat{\tau}_1$ определяет границу «неопределенного» множества $J_{\hat{\tau}_1} = \left(-\infty, \hat{\tau}_1\right)$, при попадании в которое случайной величины $\hat{\tau}_2$ индикаторы $\hat{\omega}_1$, $\hat{\omega}_2$ могут принять уже любые значения из интервала (0, 1].

Применение специализированной модели целенаправленного процесса для построения стохастических временных индикаторов

Математической моделью обнаружения СОИБ любого сценария ДВ и предъявляемых к оперативности их функционирования требований является оперативный Т-процесс [7].

С учетом вышеизложенного приведены стохастические временные индикаторы, характеризующие сценарии ДВ:

— ω_l^{τ} — стохастический супериндикатор продолжительности обнаружения $\hat{\tau}_c$ l-го АСИБ;

— $\omega_{l,l+1}^{t}$ — стохастический супериндикатор очередности обнаружения c_l^r АСИБ в составе реализующегося сценария J_m^r ДВ r-го типа на основе оценивания случайной очередности момента $\hat{t}_l^{\text{зв}}$ завершения l-го АСИБ и момента $\hat{t}_{l+1}^{\text{нч}}$ начала $(l + 1)$-й реализации следующего;

— $\overline{\omega}_{l,l+1}^{\tau}$ — стохастический супериндикатор очередности завершения обнаружения двух АСИБ на основе оценивания продолжительности $\hat{\tau}_l$, $\hat{\tau}_{l+1}$ l-го и $(l + 1)$-го воздействия соответственно.

Для удобства понимания дальнейшего изложения текста обозначим данные индикаторы символом ω_1, который носит название стохастического супериндикатора первого порядка, соответственно примем

$$\overline{\omega}_1 = P\left(\hat{\tau}' \le \hat{\tau}''\right). \tag{43}$$

С учетом сказанного показатель эффективности (ПЭ) $P_{\text{д.ц}}^1$ обнаружения сценария ДВ запишется в виде

$$P_{\text{д.ц}}^1 = P\left(\hat{\tau}' \le \hat{\tau}''\right). \tag{44}$$

В рамках методологии следует отметить, что величина $\hat{\tau}'$ представляет собой минимально необходимый целевой эффект, выраженный во временных единицах с учетом эффекта поглощения по операционным ресурсам [7].

Тогда, например, значение ПЭ $P_{\text{д.ц}}^2$ процесса функционирования СОИБ (вероятность того, что злоумышленник не реализует сценарий ДВ) определяется выражением

$$P_{\text{д.ц}}^2 = 1 - P_{\text{д.ц}}^1. \tag{45}$$

Для определения значения вероятности $P_{\text{д.ц}}^1$ необходимо и достаточно знать законы распределения случайных величин $\hat{\tau}'$ и $\hat{\tau}''$, тогда

$$P_{\text{д.ц}}^1 = P\left(\hat{\tau}' \le \hat{\tau}''\right) = P\left[\left(\hat{\tau}', \hat{\tau}''\right) \in H\right] = \iint\limits_{(H)} \varphi_{\langle \hat{\tau}', \hat{\tau}'' \rangle}(\tau', \tau'')\,d\tau' d\tau'', \tag{46}$$

где $(H) \cong \{\langle \tau', \tau'' \rangle : \tau' < \tau''\}$.

Пусть случайные величины $\hat{\tau}'$ и $\hat{\tau}''$ подчинены смещенным показательным законам распределения с параметрами соответственно λ_1, τ_1 и λ_2, τ_2, т. е.

$$F_{\hat{\tau}'}(\tau') = \left[1 - e^{-\lambda_1\left(\hat{\tau}' - \tau_1\right)}\right]\Delta\left(\hat{\tau}' - \tau_1\right). \tag{47}$$

Тогда функция $F_{\hat{\omega}_1}(\omega)$ распределения стохастического супериндикатора $\hat{\omega}_1$ принимает вид

$$F_{\hat{\omega}_1}(\omega) = F_{\hat{\tau}''}\left[F_{\hat{\tau}'}^{-1}(\omega)\right] = \left[1 - e^{-\lambda_2(\tau_1 - \tau_2)}(1 - \omega)^{\frac{\lambda_2}{\lambda_1}}\right] \times \times \prod\left(\omega;\ \sup\left\{0, F_{\hat{\tau}'}(\lambda_2)\right\}, 1\right) + \Delta(\omega - 1). \tag{48}$$

Плотность распределения

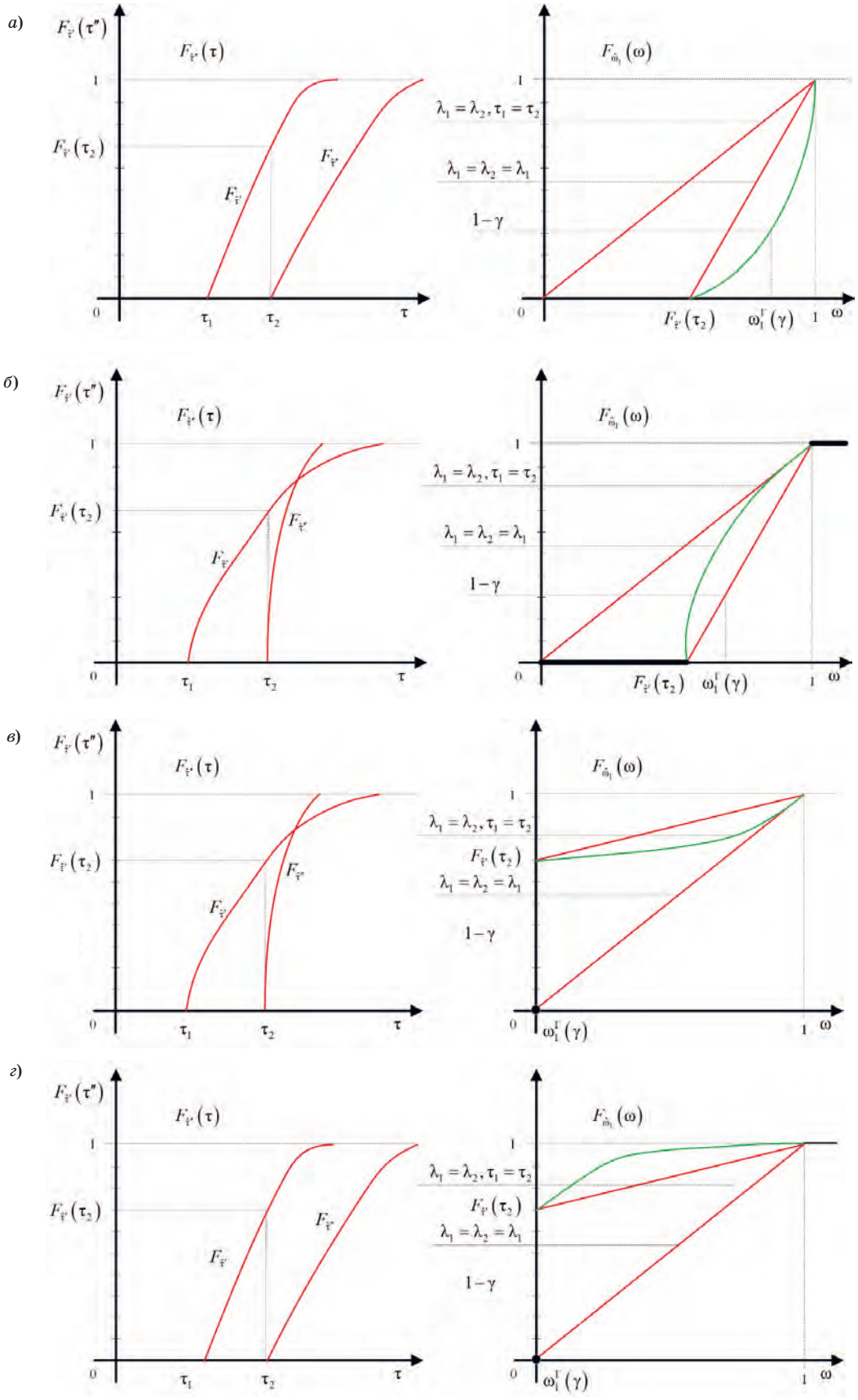
$$\varphi_{\hat{\omega}_1}(\omega) = \frac{\lambda_2}{\lambda_1} e^{\lambda_2(\tau_2 - \tau_1)} \times \times (1 - \omega)^{\frac{\lambda_2}{\lambda_1} - 1} \prod\left(\omega;\ \sup\left\{0, F_{\hat{\tau}'}(\lambda_2)\right\}, 1\right). \tag{49}$$

В результате

$$P_{\text{д.ц}}^1 = \overline{\omega}_1 = \left[1 - \frac{\lambda_2}{\lambda_2 + \lambda_1} e^{-\lambda_1(\tau_2 - \tau_1)}\right] \times \Delta(\tau_2 - \tau_1) + + \frac{\lambda_1}{\lambda_2 + \lambda_1} e^{-\lambda_2(\tau_1 - \tau_2)} \Delta(\tau_1 - \tau_2). \tag{50}$$

Тогда гарантируемая вероятность

$$\omega_1^{\Gamma} = \left[1 - \gamma^{\frac{\lambda_1}{\lambda_2}} e^{\lambda_1(\tau_1 - \tau_2)}\right] \times \times \left[\Delta(\tau_2 - \tau_1) + \Delta\left(R_{\hat{\tau}'}(\tau_1) - \gamma\right)\Delta(\tau_1 - \tau_2)\right], \tag{51}$$



■ ***Рис. 6.*** Функции $F_{\hat{\omega}_1}(\omega)$ для первого (*а*), второго (*б*), третьего (*в*) и четвертого (*г*) случая

■ ***Fig. 6.*** The functions $F_{\hat{\omega}_1}(\omega)$ for the first (*а*), second (*б*), third (*в*), and fourth (*г*) cases

где γ — уровень гарантии (гарантийная вероятность).

В зависимости от соотношений параметров τ_1, τ_2 и λ_1, λ_2 функция распределения $F_{\hat{\omega}_1}(\omega)$ стохастического супериндикатора $\hat{\omega}_1$ принимает конкретный вид, соответствующий одному из четырех вариантов:

1) $\tau_1 < \tau_2$, $\lambda_1 > \lambda_2$;
2) $\tau_1 < \tau_2$, $\lambda_1 < \lambda_2$;
3) $\tau_1 > \tau_2$, $\lambda_1 < \lambda_2$;
4) $\tau_1 > \tau_2$, $\lambda_1 > \lambda_2$.

В частности, если $\tau_1 < \tau_2 \wedge (\lambda_1 > \lambda_2 \vee \lambda_1 < \lambda_2)$, то для случаев 1) и 2) функция распределения $F_{\hat{\omega}_1}(\omega)$ стохастического супериндикатора $\hat{\omega}_1$ примет вид

$$F_{\hat{\omega}_1}(\omega) = \left[1 - e^{\lambda_2(\tau_2-\tau_1)}(1-\omega)^{\frac{\lambda_2}{\lambda_1}}\right] \times \times \prod\left(\omega;\, F_{\hat{\tau}'}(\tau_2),\, 1\right) + \Delta(\omega - 1); \quad (52)$$

$$\varphi_{\hat{\omega}_1}(\omega) = \frac{\lambda_2}{\lambda_1} e^{\upsilon(\tau_2-\tau_1)} \times \times (1-\omega)^{\frac{\lambda_2}{\lambda_1}-1} \prod\left(\omega;\, F_{\hat{\tau}'}(\tau_2),\, 1\right); \quad (53)$$

$$\bar{\omega}_1 = 1 - \frac{\lambda_2}{\lambda_2 + \lambda_1} e^{\lambda_1(\tau_1-\tau_2)}; \quad (54)$$

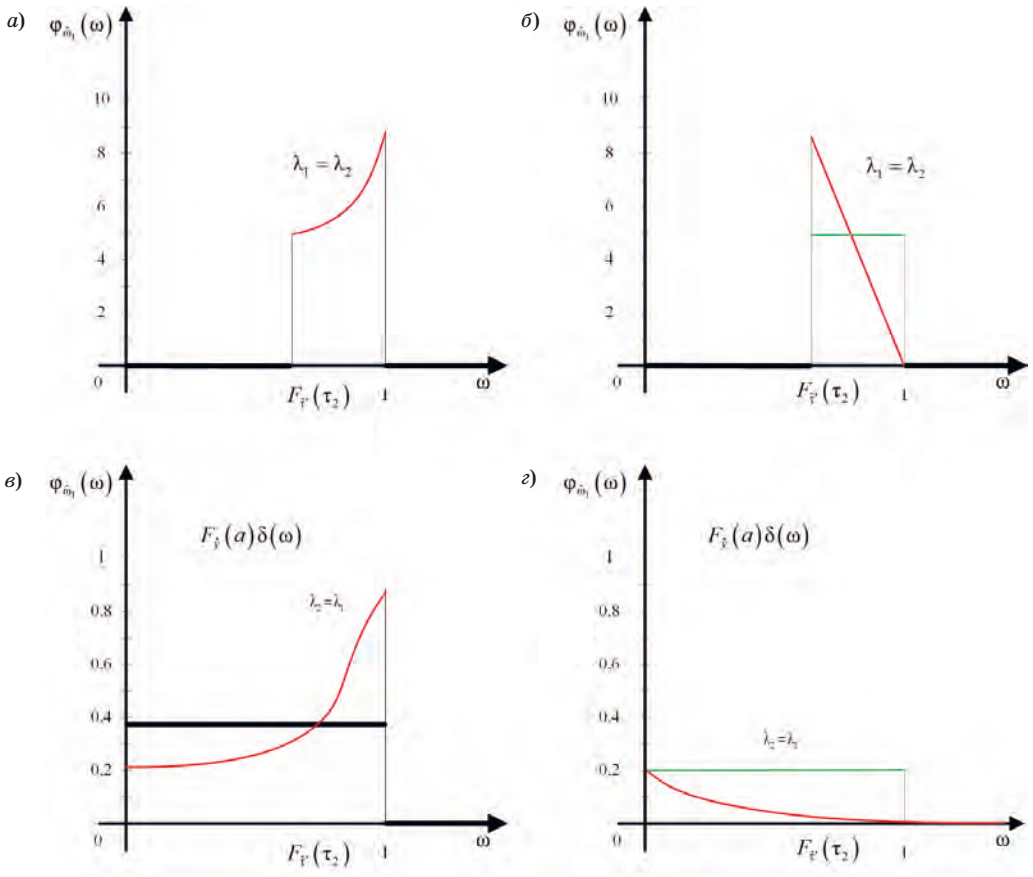
$$\omega_1^{\Gamma}(\gamma) = 1 - \gamma^{\frac{\lambda_1}{\lambda_2}} e^{\lambda_1(\tau_1-\tau_2)}. \quad (55)$$

Для случаев 3) и 4) при условии $\tau_1 > \tau_2 \wedge \wedge (\lambda_1 < \lambda_2 \vee \lambda_1 > \lambda_2)$ функция распределения $F_{\hat{\omega}_1}(\omega)$ стохастического супериндикатора $\hat{\omega}_1$ примет вид

$$F_{\hat{\omega}_1}(\omega) = = \left[1 - e^{\lambda_2(\tau_2-\tau_2)}(1-\omega)^{\frac{\lambda_2}{\lambda_1}}\right] \prod(\omega;\, 0,1) + + \Delta(\omega - 1); \quad (56)$$

$$\varphi_{\hat{\omega}_1}(\omega) = = \frac{\lambda_2}{\lambda_1} e^{\lambda_2(\tau_2-\tau_1)}(1-\omega)^{\frac{\lambda_2}{\lambda_1}-1} \prod(\omega;\, 0,1) + + F_{\hat{\tau}''}(\tau_1)\delta(\omega); \quad (57)$$

$$\bar{\omega}_1 = 1 - \frac{\lambda_1}{\lambda_1 + \lambda_2} e^{\lambda_2(\tau_2-\tau_1)}; \quad (58)$$



■ ***Рис. 7.*** Кривые распределения индикатора $\hat{\omega}_1$ для первого (*а*), второго (*б*), третьего (*в*) и четвертого (*г*) случая
■ ***Fig. 7.*** Distribution curves of the indicator $\hat{\omega}_1$ for the first (*а*), second (*б*), third (*в*), and fourth (*г*) cases

$$\omega_1^{\Gamma}(\gamma)=\left[1-\gamma^{\frac{\lambda_1}{\lambda_2}e^{\lambda_1(\tau_1-\tau_2)}}\right]\Delta\left(F_{\hat{\tau}'}(\tau_1)-\gamma\right). \quad (59)$$

Графики функции $F_{\hat{\omega}_1}(\omega)$ для случаев 1) и 2), когда значения параметров τ_1, τ_2 и λ_1, λ_2 исходных распределений $F_{\hat{\tau}'}(\tau')$ и $F_{\hat{\tau}''}(\tau'')$ совпадают и $\lambda_1=\lambda_2=\lambda_1$, приведены на рис. 6, *а* и *б*.

При совпадении исходных распределений $F_{\hat{\tau}''}(\tau'')$ значений параметров τ_1, τ_2 и λ_1, λ_2 функции $F_{\hat{\omega}_1}(\omega)$ и при $\lambda_2=\lambda_1=\lambda_2$, для случаев 3) и 4) существует обратная зависимость относительно случая 1) и 2), которая отображена на рис. 6, *в* и *г*.

Кривые распределения индикатора $\hat{\omega}_1$ для всех указанных случаев приведены на рис. 7, *а–г*.

Действительно, в зависимости от соотношений параметров τ_1, τ_2 и λ_1, λ_2 функция распределения $F_{\hat{\omega}_1}(\omega)$ стохастического супериндикатора $\hat{\omega}_1$ принимает конкретный вид, соответствующий одному из четырех приведенных выше вариантов.

Заключение

Исследование эффективности процесса функционирования СОИБ комплексно и корректно может быть осуществлено только на методологической основе современной теории эффективности целенаправленных процессов. В этом случае исследователю удается учесть весь комплекс результатов процесса функционирования системы — как положительных (объем и качество целевого эффекта), так и отрицательных (расходы ресурсов и времени).

Разработан подход к оцениванию эффективности процессов функционирования системы обеспечения информационной безопасности на основе теории стохастической индикации, призванной служить инструментом вероятностного анализа случайных явлений.

Формализована стохастическая ситуация для количественного анализа исследования процессов функционирования систем обеспечения информационной безопасности. Рассмотрены основные свойства стохастических индикаторов. Построены стохастические временные индикаторы на основе специализированной модели целенаправленного процесса.

При решении задач исследования эффективности следует использовать специфичные агрегированные модели системы, которые отражают с требуемой адекватностью результаты процесса их функционирования, динамику их получения в ходе операции и их связи с параметрами и эксплуатационно-техническими характеристиками СОИБ и ее процессом функционирования, без детального описания всех элементов системы.

Литература

1. **Daraio C., Simar L.** *Advanced Robust and Nonparametric Methods in Efficiency Analysis: Methodology and Applications.* Springer, 2007. 263 p.
2. **Зуев М. Б., Зуев Б. П., Булгакова И. Н.** Усовершенствованный метод освоенного объема для интегральной оценки эффективности и прогнозов результата деятельности в сфере управления. *Управление проектами: идеи, ценности, решения: материалы I Междунар. науч.-практ. конф.*, Санкт-Петербург, 15–17 мая 2019 г. СПб., СПбГАСУ, 2019, с. 80–87.
3. **Юсупов Р. М., Мусаев А. А.** Особенности оценивания эффективности информационных систем и технологий. *Тр. СПИИРАН*, 2017, вып. 1(51), с. 5–34. doi:10.15622/sp.51.1
4. **Арсеньев В. Н., Хомоненко А. Д., Ядренкин А. А.** Взвешенный учет априорной и опытной информации в задаче оценивания эффективности функционирования системы управления при распределении числа испытаний по закону Паскаля. *Информационно-управляющие системы*, 2020, № 3, с. 39–47. doi:10.31799/1684-8853-2020-3-39-47
5. **Беляков М. И.** Модель процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры в задаче оценивания его эффективности. *Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму*, 2020, № 11-12 (149-150), с. 71–75.
6. **Wetering V., Mikalef P., Adamantia P.** A strategic alignment model for IT flexibility and dynamic capabilities: Toward an assessment tool. *Twenty-Fifth European Conf. on Information Systems (ECIS)*, 2017, pp. 1–17.
7. **Петухов Г. Б., Якунин В. И.** *Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем*. М., АСТ, 2006. 504 с.
8. **Фролов О. П., Кузьмин В. Н., Зиннуров С. Х.** Методологический подход к решению слабоформализуемых задач оценивания эффективности и выбора рациональных способов применения космических систем. *Изв. Российской академии ракетных и артиллерийских наук*, 2020, № 3 (113), с. 59–65.
9. **Галанкин А. В., Гончаров А. М., Чащин С. В.** Оценивание эффективности функционирования цифровой сети связи космических войск. *Тр. Военно-космической академии им. А. Ф. Можайского*, 2016, № 650, с. 7–10.

10. **McMahon P.** *15 Fundamentals for Higher Performance in Software Development: Includes discussions on CMMI, Lean Six Sigma, Agile and SEMAT's Essence Framework*. Pem Systems Publ., 2014. 336 p.
11. **Гейда А. С., Лысенко И. В., Юсупов Р. М.** Основные концепты и принципы исследования операционных свойств использования информационных технологий. *Тр. СПИИРАН*, 2015, вып. 5(42), с. 5–36. doi:10.15622/sp.42.1
12. **Гейда А. С., Исмаилова З. Ф., Клитный И. В., Лысенко И. В.** Задачи исследования операционных и обменных свойств систем. *Тр. СПИИРАН*, 2014, вып. 4(35), с. 136–160. doi:10.15622/sp.35.10
13. **Schilke O., Hu S., Helfat C.** Quo vadis, dynamic capabilities? A content-analytic review of the current state of knowledge and recommendations for future research. *Academy of Management Annals*, 2018, vol. 12, no. 1, pp. 390–439.
14. **Garza-Reyes J.** From measuring overall equipment effectiveness (OEE) to overall resource effectiveness (ORE). *Journal of Quality in Maintenance Engineering*, 2015, vol. 21(4), pp. 506–527.
15. **Сухов А. М., Крупенин А. В., Якунин В. И.** Методы анализа и синтеза исследования эффективности процессов функционирования системы обнаружения предупреждения и ликвидации последствий компьютерных атак. *Автоматизация процессов управления*, 2021, № 4 (66), с. 4–14.
16. **Сухов А. М., Герасимов С. Ю., Еремеев М. А., Якунин В. И.** Математическая модель процесса функционирования подсистемы реагирования системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. *Проблемы информационной безопасности. Компьютерные системы*, 2019, № 2, с. 56–64.
17. **Браницкий А. А., Котенко И. В.** Анализ и классификация методов обнаружения сетевых атак. *Тр. СПИИРАН*, 2016, вып. 2(45), с. 207–244. doi:10.15622/SP.45.13
18. **Юрчик П. Ф., Андрющенко В. И., Шастин С. Д.** Формирование архитектуры единого информационного пространства. *Школа Науки*, 2021, № 1 (38), с. 33–36.
19. **Горбачев И. Е., Сухов А. М., Еремеев М. А., Смирнов С. И.** Методика реализации системного подхода при создании облика системы информационной безопасности критической информационной инфраструктуры с учетом экономической целесообразности. *Проблемы информационной безопасности. Компьютерные системы*, 2018, № 2, с. 93–110.
20. **Сухов А. М., Ступин Д. Д., Ломако А. Г.** Модель проактивного обнаружения компьютерных атак. *Проблемы управления и моделирования в сложных системах: тр. XX Междунар. конф.*, Самара, 3–6 сентября 2018 г.; под ред. Е. А. Федосова, Н. А. Кузнецова, С. Ю. Боровика. Самара, 2018, с. 509–512.
21. **Маликов А. В., Авраменко В. С., Саенко И. Б.** Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении. *Информационно-управляющие системы*, 2019, № 6, с. 32–42. doi:10.31799/1684-8853-2019-6-32-42

UDC 519.718
doi:10.31799/1684-8853-2022-3-31-44

Evaluating the effectiveness of the information security system process based on the theory of stochastic indicators

A. M. Sukhov[a], PhD, Tech., Doctoral Candidate, orcid.org/0000-0003-2233-811X, 19am87@mail.ru
[a]Krasnodar Higher Military School named after General of the Army S. M. Shtemenko, 4, Krasin St., 350065, Krasnodar, Russian Federation

Introduction: Under the conditions of imperfect methods and means of detection and response to computer attacks there is a constant growth of destructive impacts aimed at critical information systems. This generates a need to develop research methods for early warning systems to provide information security in case of malware attacks. One of the effective ways to solve this problem is to use the methods of the theory of stochastic indicators. **Purpose:** The development of a tool for evaluating the effectiveness of the information security system functioning. **Results:** We describe deterministic, random and indefinite components of the information security system functioning. Constant and functional indicators are constructed, their distinctive features are revealed. To solve the problem of evaluating the effectiveness of the process under consideration stochastic superindicators are constructed. We have also described the features of the construction of stochastic indicators of different ranks on the basis of the theory of the effectiveness of targeted processes and purposeful systems. **Practical relevance:** Through the developed stochastic time indicators, the probabilistic and temporal characteristics of the destructive impact are estimated, with the intervals and time points of its occurrence taken into account. This allows the system to be timely warned of a possible destructive impact scenario for the elements of critical information infrastructure.

Keywords — information security system, atomic information security event, destructive impact, efficiency, quality, stochastic indication theory.

For citation: Sukhov A. M. Evaluating the effectiveness of the information security system process based on the theory of stochastic indicators. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 31–44 (In Russian). doi:10.31799/1684-8853-2022-3-31-44

References

1. Daraio C., Simar L. *Advanced Robust and Nonparametric Methods in Efficiency Analysis: Methodology and Applications*. Springer, 2007. 263 p.
2. Zuev M. B., Zuev B. P., Bulgakova I. N. Upgraded method of the mastered volume for integrated assessment of efficiency and forecasts of result of activity in the management. *Materialy 1-j Mezhdunarodnoj nauchno-prakticheskoj konferencii "Upravlenie proektami: idei, cennosti, resheniya"* [Proc. 1st Intern. Scient. and Pract. Conf. "Project management: ideas, values, solutions"]. Saint-Petersburg, 2019, pp. 80–87 (In Russian).
3. Yusupov R. M., Musaev A. A. Efficiency of information systems and technologies: Features of estimation. *SPIIRAS Proc.*, 2017, vol. 2, no. 51, pp. 5–34 (In Russian). doi:10.15622/sp.51.1
4. Arseniev V. N., Khomonenko A. D., Yadrenkin A. A. Weighed ranking of aprioristic and experimental data in control system functioning efficiency estimation problem with Pascal-distributed number of tests. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 3, pp. 39–47 (In Russian). doi:10.31799/1684-8853-2020-3-39-47
5. Belyakov M. I. Model of the process of functioning of the information security system of a critical information infrastructure object in the assessment of its effectiveness. *Military Enginery. Iss. 16: Counter-terrorism technical devices*, 2020, no. 11-12 (149-150), pp. 37–40 (In Russian).
6. Mikalef P., Adamantia P. A strategic alignment model for IT flexibility and dynamic capabilities: Toward an assessment tool. *Twenty-Fifth European Conference on Information Systems (ECIS)*, 2017, pp. 1–17.
7. Petukhov G. B., Yakunin V. I. *Metodologicheskie osnovy vneshnego proektirovaniya celenapravlennyh processov i celeustremlennyh sistem* [Methodological basis of external designing of targeted processes and purposeful systems]. Moscow. AST Publ., 2006. 504 p. (In Russian).
8. Frolov O. P., Kuzmin V. N., Zinnurov S. H. Methodological approach to solving poorly formalized problems of evaluating the effectiveness and choosing rational ways of using space systems. *Izvestiya Rossijskoj akademii raketnyh i artillerijskih nauk*, 2020, no. 3 (113), pp. 59–65 (In Russian).
9. Galankin A. V., Goncharov A. M., Chashchin S. V. Evaluation of the effectiveness of the functioning of the digital communication network of the space forces. *Proc. of the Mozhaisky Military Space Academy*, 2016, no. 650, pp. 7–10 (In Russian).
10. McMahon P. *15 Fundamentals for Higher Performance in Software Development: Includes discussions on CMMI, Lean Six Sigma, Agile and SEMAT's Essence Framework*. Pem Systems Publ., 2014. 336 p.
11. Geida A. S., Lysenko I. V., Yusupov R. M. Main concepts and principles for information technologies operational properties research. *SPIIRAS Proc.*, 2015, vol. 5, no. 42, pp. 5–36 (In Russian). doi:10.15622/sp.42.1
12. Geida A. S., Ismailova Z. F., Klitnuy I. V., Lysenko I. V. Operational and exchange properties of systems research problems. *SPIIRAS Proc.*, 2014, vol. 4, no. 35, pp. 136–160 (In Russian). doi:10.15622/sp.35.10
13. Schilke O., Hu S., Helfat C. Quo vadis, dynamic capabilities? A content-analytic review of the current state of knowledge and recommendations for future research. *Academy of Management Annals*, 2018, vol. 12, no. 1, pp. 390–439.
14. Garza-Reyes J. From measuring overall equipment effectiveness (OEE) to overall resource effectiveness (ORE). *Journal of Quality in Maintenance Engineering*, 2015, vol. 21(4), pp. 506–527.
15. Sukhov A. M., Krupenin A. V., Yakunin V. I. The analysis and synthesis methods of research of the operation processes efficiency of the computer attacks detection, prevention and consequences elimination system. *Automated Control Systems*, 2021, no. 4 (66), pp. 4–14 (In Russian).
16. Sukhov A. M., Gerasimov S. Yu., Eremeev M. A., Yakunin V. I. Mathematical model of the process of functioning of detection system prevention and mitigation of computer attacks. *Information Security Problems. Computer Systems*, 2019, no. 2, pp. 56–64 (In Russian).
17. Branitskiy A. A., Kotenko I. V. Analysis and classification of methods for network attack detection. *SPIIRAS Proc.*, 2016, vol. 2, no. 45, pp. 207–244 (In Russian). doi:10.15622/SP.45.13
18. Yurchik P. F., Andryushchenko V. I., Shastin S. D. Formation of the architecture of a single information space. *School of Science*, 2021, no. 1 (38), pp. 33–36 (In Russian).
19. Gorbachev I. E., Sukhov A. M., Eremeev M. A., Smirnov S. I. The implementation of a systematic approach in creation of system of information security of critical information infrastructure taking into account economic feasibility. *Information Security Problems. Computer Systems,* 2018, no. 2, pp. 93–110 (In Russian).
20. Sukhov A. M., Stupin D. D., Lomako A. G. A model of proactive detection of computer attacks. *Trudy XX Mezhdunarodnoj konferencii "Problemy upravleniya i modelirovaniya v slozhnyh sistemah". Pod redakciej E. A. Fedosova, N. A. Kuznecova, S. Yu. Borovika* [Proc. of the XX Intern. Conf. "Complex systems: Control and modeling problems"]. Samara, 2018, pp. 509–512 (In Russian).
21. Malikov A. V., Avramenko V. S., Saenko I. B. Model and method for diagnosing computer incidents in information and communication systems based on deep machine learning. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 6, pp. 32–42 (In Russian). doi:10.31799/1684-8853-2019-6-32-42