УДК 519.87(075.8)

Е.С. Щербаков[1]
П.В. Корчагин[2]

ОСОБЕННОСТИ УЧЁТА СТАТИСТИЧЕСКОГО ХАРАКТЕРА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В статье дано эмпирико-теоретическое обоснование необходимости применения теории возможностей для корректного учёта статистической неопределённости, характеризующей функционирование систем защиты информации (СЗИ).

Ключевые слова: *информационная защита, защищаемый объект, фактор неопределённости, эксперимент, вероятность обнаружения.*

E.S. Shcherbakov
P.V. Korchagin

INFORMATION SECURITY SYSTEMS: SOME STATISTICAL FEATURES IN ACCOUNTING THEIR FUNCTIONS

The article gives the empirical and theoretical justification for the need to applicate the theory of opportunities for correct accounting of the statistical uncertainty, that characterizes the operation of information security systems.

Keywords: *information protection, protected object, factor of uncertainty, experiment, probability of detection.*

Информационная защита устройств электронной вычислительной и коммуникационной техники (УЭВКТ) основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от несанкционированного доступа (НСД) к информации и, прежде всего, положениям, изложенным в Доктрине [1].

Если в текущий момент времени на вход УЭВКТ воздействует *k*-й источник информационных угроз, то СЗИ с задержкой по времени $T_{зад}^{СЗИ}$ нейтрализует угрозы с вероятностью, определяемой на этапе сертификации СЗТ. Для эффективного функционирования защищаемого объекта необходимо одновременное выполнение двух условий:

− во-первых, СЗИ *j*-го типа должна обеспечивать защиту информации с вероятностью не ниже требуемой вероятности обнаружения и нейтрализации угрозы *i*-го типа:

$$\forall_i \in I \wedge \forall_j \in J \; P_{ij}^{СЗИ} \geq P_i^{треб}, \quad (1)$$

где *I* – множество типов информационных угроз;

J – множество типов СЗИ, использование которых допустимо на защищаемом объекте;

$P_{ij}^{СЗИ}$ – эффективность защиты информации с помощью СЗИ *j*-го типа при нейтрализации угрозы *i*-го типа;

$P_i^{треб}$ – требуемая эффективность защиты информации от угрозы *i*-го типа;

− во-вторых, время задержки выполнения *k*-ой функции системы, обусловленное применением СЗИ *j*-го типа, должно быть меньше допустимого:

$$\tau_{ijk}^{задерж} \leq \tau_к^{ДОП}, \quad (2)$$

где $\tau_{ijk}^{задерж}$ – время задержки выполнения *k*-ой функции защищаемого объекта, обусловленное применением СЗИ *j*-го типа при угрозе *i*-го типа;

$\tau_к^{ДОП}$ – допустимое время задержки выполнения *k*-ой функции защищаемого объекта, то есть время задержки, несущественно влияющее на эффективность функционирования защищаемого объекта, например КСА КП частей и соединений ВКС.

В ходе испытаний УЭВКТ, входящих в состав аппаратуры КП частей и соединений ВКС, проводится проверка выполнения условия (2). Проведение указанной проверки сопряжено с

[1] Кандидат технических наук, профессор Военной академии воздушно-космической обороны, г. Тверь.

[2] Кандидат технических наук, Военно-космическая академия, г. Санкт-Петербург.

наличием существенного фактора неопределённости. Дело в том, что величина $\tau_{jk}^{задерж}$ является случайной и существенно зависит от условий обстановки, в которой реализуется выполнение *k*-ой функции системы УЭВКТ. Поэтому можно говорить о вероятности выполнения условия (2).

В ходе испытаний достаточно просто оценить среднее значение величины задержки по формуле:

$$\overline{\tau}_{jk}^{задерж} = \frac{1}{N_{jk}} \sum_{n=1}^{N_{jk}} \overline{\tau}_{jkn}^{задерж}, \qquad (3)$$

где $\overline{\tau}_{jk}^{задерж}$ – среднее значение величины $\tau_{jk}^{задерж}$, полученное в ходе испытаний;

$\overline{\tau}_{jkn}^{задерж}$ – оценка значения $\tau_{jk}^{задерж}$, полученная в ходе *n*-го эксперимента в процессе испытаний;

N_{jk} – количество экспериментов, связанных с оценкой $\overline{\tau}_{jk}^{задерж}$ в ходе испытаний.

Но так как величина $\tau_{jk}^{задерж}$ является случайной и существенно зависит от контекста обстановки, то реально условие (2) может интерпретироваться только с помощью вероятностной оценки:

$$\widehat{Э}_{ijk} = \widehat{P}_{ijk}^{гарант}(\tau_{jk}^{задерж} \le \tau_{к}^{доп} \mid P_{ij}^{СЗИ} \ge P_{i}^{треб}), \qquad (4)$$

где $\widehat{Э}_{ijk}$ – оценка эффективности СЗИ *j*-го типа при обслуживании функции УЭВКТ *k*-го типа;

$\widehat{P}_{ijk}^{гарант}(...)$ – оценка гарантированной условной вероятности выполнения условия (2) при выполнении условий (1) и (2).

Так как одно и то же СЗИ (или комплекс СЗИ) используется для защиты УЭВКТ, выполняющих широкий спектр функций, то возникает необходимость формирования интегрального показателя эффективности *j*-го типа СЗИ. В качестве такого показателя может использоваться следующий:

$$Э_{k}^{интегр} = \max_{\forall i \in I \wedge \forall j \in J}(\widehat{Э}_{11k}, \widehat{Э}_{21k}, \ldots \widehat{Э}_{ijk}), \qquad (5)$$

где $Э_{k}^{интегр}$ – интегральная оценка эффективности *k*-го СЗИ.

Приведённый порядок оценки эффективности функционирования СЗИ на первый взгляд кажется вполне элементарным и не вызывающим принципиальных трудностей. Однако главная методологическая трудность в реализации предложенного подхода кроется в оценке вероятности $\widehat{P}_{ijk}^{гарант}(...)$. Для расчёта указанной вероятности требуется знать закон распределения оценки случайной величины времени задержки $\tau_{jk}^{задерж}$. К сожалению, практика определения указанного закона характеризуется одним неприятным обстоятельством, а именно: при условии выбора в качестве априорных гипотез одного из законов распределения (рис. 1) исследователь сталкивается с ситуацией, когда при использовании критерия Пирсона (x^2-*критерия*) при заданной вероятности ошибки второго рода меньшей 0,1 ни один из законов не адекватен статистическим данным. Зато при заданной вероятности ошибки второго рода не меньшей 0,3 все приведённые выше законы становятся вполне адекватными, но, одновременно с этим, дают принципиально отличающиеся друг от друга оценки (5). Наращивание количества экспериментальных данных ситуацию не исправляет. Представленные данные свидетельствуют о том, что время задержки является величиной неопределённой, но не подчиняется закону больших чисел. Стабилизации экспериментального закона распределения при росте количества реализаций не происходит. Данное обстоятельство свидетельствует о том, что сами оценки параметров случайных величин $\tau_{jk}^{задерж}$ не соответствуют аксиомам Колмогорова, определяющих понятие «случайная величина». То есть, величина $\tau_{jk}^{задерж}$ является неопределённой, но закон её распределения не может быть выявлен.

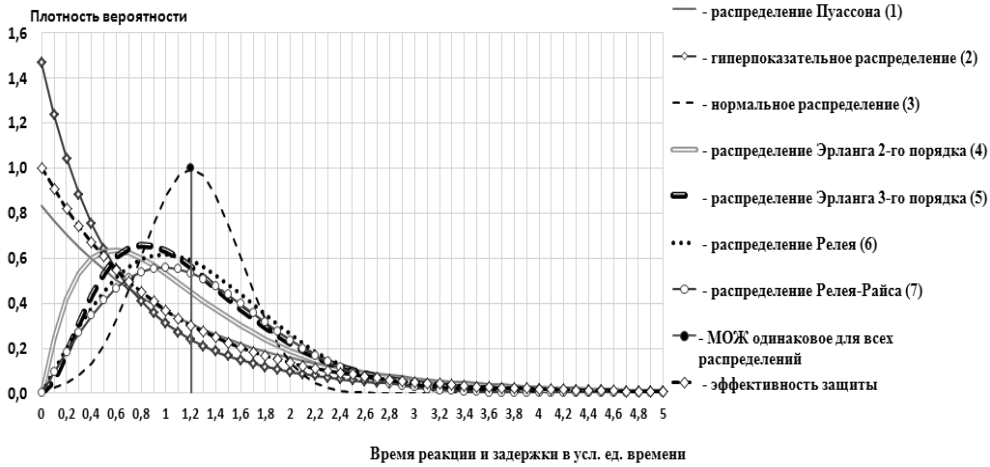

Рис. 1. Графики типовых законов распределения, наиболее адекватно описывающих экспериментальные распределения величины времени задержки $\tau_{jk}^{задерж}$

Результаты экспериментальных исследований оценок времени задержки ставят под сомнение целесообразность применения вероятностных методов при исследовании свойств систем защиты информации и указывает на необходимость использования для исследования факторов неопределённости, сопряжённых с исследованием свойств систем защиты информации альтернативных методов, например методов теории возможностей [2].

Литература

1. Доктрина информационной безопасности Российской Федерации. // Российская газета. – 2000. – 28 сентября.

2. Пытьев Ю.П. Возможность как альтернатива вероятности. Математические и эмпирические основы, применение. – М. : ФИЗМАТЛИТ, 2007.