Управление рисками и безопасностью

Подход к оценке эффективности мероприятий по комплексной защите информационных ресурсов

В. В. Александров, А. П. Котельников

Аннотация. Решение задач по защите информации должно осуществляться системно, на основе анализа существующих подходов к обеспечению информационной безопасности. Эти подходы представляют собой целенаправленную систему мероприятий по выявлению и предотвращению преступных посягательств на информационные ресурсы. Целью исследования является разработка математической модели для оценки эффективности мероприятий по комплексной защите информационных ресурсов. Аналитическая модель позволяет получить численные значения показателей эффективности комплексной защиты информационных ресурсов.

Ключевые слова: *математическая модель, защита информации, комплексная защита информации.*

В связи со стремительным прогрессом в области сетевых технологий, телекоммуникаций и новых информационных технологий стали актуальными проблемы защиты информации, задачи противодействия преступлениям в отношении информационных ресурсов. Их решение должно осуществляться системно, на основе всестороннего анализа существующих подходов к обеспечению информационной безопасности. Эти подходы представляют собой целенаправленную систему мероприятий по выявлению и предотвращению преступных посягательств на информационные ресурсы.

Таким образом, возникает необходимость разработки системных методик по оценке эффективности мероприятий по комплексной защите информационных ресурсов, учитывающих все особенности реализуемых при этом функций защиты информации.

Как показывает анализ состояния проблемы, одним из наиболее перспективных путей ее решения является интегрирование отдельных частных показателей эффективности выполняемых функций по выявлению и предотвращению преступных посягательств на информационные ресурсы в единый комплексный показатель.

Целью данной работы является разработка математической модели для оценки эффективности мероприятий по комплексной защите информационных ресурсов.

Определим функции защиты информации Fn_i как кортеж:

$$Fn_i = \langle Id_i,\ Mod_i,\ \Psi_i \rangle,$$

где Id_i — идентификатор i-й функции;

Mod_i — структурированное множество программных модулей, реализующих i-ю функцию;

Ψ_i — характеристика объема рабочей среды программных средств, реализующих i-ю функцию противодействия угрозам безопасности, представимая, в свою очередь, в виде кортежа:

$$\Psi_i = \langle \psi_i^{(1)}, \psi_i^{(2)}, \psi_i^{(3)}, \psi_i^{(4)} \rangle, \qquad (1)$$

где $\psi_i^{(1)}$, $\psi_i^{(2)}$, $\psi_i^{(3)}$ и $\psi_i^{(4)}$ — характеристики случайной величины объема рабочей среды программных средств, реализующих i-ю функцию:

$\psi_i^{(1)}$ — условное обозначение закона распределения [2] случайной величины объема рабочей среды программных средств, реализующих i-ю функцию (равномерный, усеченный экспоненциальный, усеченный нормальный);

$\psi_i^{(2)}$ — при усеченных экспоненциальном и нормальном законах распределения — среднее значе-

ние случайной величины объема рабочей среды программных средств, реализующих i-ю функцию, при равномерном — минимальное значение;

$\psi_i^{(3)}$ — при усеченном нормальном законе распределения — среднеквадратическое отклонение случайной величины объема рабочей среды программных средств, реализующих i-ю функцию, при усеченном экспоненциальном — минимальное значение, при равномерном — максимальное;

$\psi_i^{(4)}$ — минимальное значение случайной величины объема рабочей среды программных средств, реализующих i-ю функцию при усеченном нормальном законе распределения.

На множестве $\{Fn_i\}$ $(i = 1,2,\ldots,I, \quad I = |\{Fn_i\}|)$ функций определим отношение зацепленности между ними и опишем его матрицей вероятностей переходов $||P||$, определяющей порядок следования функций.

Множество Mod_i программных модулей, создающих рабочую среду для реализации функции Fn_i, формально представляется в виде массива $||\Omega_i||$ характеристик их объема размерностью $|Mod_i| \times 4$. Каждая j-я строка матрицы $(j = 1, 2, \ldots, |Mod_i|)$ имеет вид:

$$\Omega_{ij} = \left\langle \omega_{ij}^{(1)}, \omega_{ij}^{(2)}, \omega_{ij}^{(3)}, \omega_{ij}^{(4)} \right\rangle, \qquad (2)$$

где $\omega_{ij}^{(1)}$, $\omega_{ij}^{(2)}$, $\omega_{ij}^{(3)}$ и $\omega_{ij}^{(4)}$ — характеристики случайной величины объема рабочей среды j-го программного модуля, реализующего i-ю функцию:

$\omega_{ij}^{(1)}$ – условное обозначение закона распределения случайной величины объема рабочей среды j-го программного модуля (равномерный, усеченный экспоненциальный, усеченный нормальный);

$\omega_{ij}^{(2)}$ – при усеченных экспоненциальном и нормальном законах распределения — среднее значение случайной величины объема рабочей среды j-го программного модуля, при равномерном — минимальное значение;

$\omega_{ij}^{(3)}$ – при усеченном нормальном законе распределения — среднеквадратическое отклонение случайной величины объема рабочей среды j-го программного модуля, при усеченном экспоненциальном — минимальное значение, при равномерном — максимальное;

$\omega_{ij}^{(4)}$ – минимальное значение случайной величины объема рабочей среды j-го программного модуля при усеченном нормальном законе распределения.

Определим на множестве (2) отношение операционной зацепленности между программными модулями $mod_{ij} \in Mod_i$, $j = 1, 2, \ldots, |Mod_i|$ и опишем его с помощью матрицы вероятностей переходов $||p_i||$, структура которой аналогична структуре матрицы $||P||$. Геометрическим эквивалентом матричного описания отношений является ориентированный граф. Имитация смены состояний ориентированного графа, в соответствии с порядком вызова для выполнения программных модулей, определяемым матрицей вероятностей переходов $||p_{ij}||$, позволяет сформировать множество $C_{(q)}$ состояний, составляющих q-ю реализацию модели [3], что, в свою очередь, позволяет определить значение объема рабочей среды программных средств, реализующих функцию противодействия угрозам безопасности, соответствующее данной реализации модели.

С целью построения аналитической модели для получения численных значений показателей эффективности комплексной защиты информационных ресурсов воспользуемся представленным в [4] методическим подходом, основанном на сходстве формы показателя вида $P(a > b)$ и классической функции распределения вероятностей.

Меры защиты информации в рамках конкретного n-го этапа возможных противоправных действий в отношении информационных ресурсов считаются реализованными адекватно, если объем $v_n^{(2)}$ рабочей среды программных средств реализующих данный этап не менее некоторой минимально допустимой величины $v_{(\min)\,n}^{(2)}$, обусловленной спецификой угроз, т. е. при выполнении неравенства [1]:

$$v_n^{(2)} \geqslant v_{(\min)\,n}^{(2)}, \qquad (3)$$

Так как объем $v_n^{(2)}$ является функцией от характеристик объема рабочей среды программных средств, реализующих соответствующие функции защиты информации, имеет место выражение:

$$v_n^{(2)} = \sum_{c=1}^{C} \circ v_c^{(1)}, \qquad (4)$$

где $v_c^{(1)}$ — объем рабочей среды программных средств реализующих c-ю функцию, а операция $\sum_{c=1}^{C} \circ$ означает композицию C случайных величин.

Минимальный объем $v_{(min)n}^{(2)}$ обусловлен спецификой воздействия угрозы противоправных действий и определяется конкретными вариантами их реализации.

Входящая в (3) величина $v_n^{(2)}$ является случайной. Вероятность события

$$P = P\left(v_n^{(2)} \geqslant v_{(min)\,n}^{(2)}\right) \qquad (5)$$

представляет собой среднее количество ситуаций, когда n-й этап мероприятий по защите информационных ресурсов реализовывался адекватно, относительно общего числа таких ситуаций, т. е. имеет место соотношение:

$$P = P\left(v_n^{(2)} \geqslant v_{(\min)\,n}^{(2)}\right) = \frac{1}{G}\sum_{g=1}^{G} \alpha_{n,\,g},$$

где $\alpha_{n\,g} = \begin{cases} 1, & \text{при } v^{(2)}_{n\,g} \geqslant v^{(2)}_{(\min)\,n\,g} \\ 0, & \text{при } v^{(2)}_{n\,g} < v^{(2)}_{(\min)\,n\,g} \end{cases}$;

$v^{(2)}_{ng}$ — объем рабочей среды программных средств реализующих n-й этап противодействия g-й, $g = 1, 2, \ldots, G$, угрозе противоправных действий;

$v^{(2)}_{(min)cg}$ — минимально допустимый объем, соответствующий g-ой угрозе при реализации n-го этапа мероприятий по защите информации;

G — общее число исследуемых ситуаций возникновения угроз противоправных действий в отношении информационных ресурсов.

В условии (3) не всегда варьируемым измеряемым параметром является объем $v^{(2)}_{n}$. В некоторых случаях измеряемым параметром может являться объем $v^{(2)}_{(min)\,n}$. В этом случае вероятность (5) примет вид:

$$\mathrm{P} = P\left(v^{(2)}_{n} \geqslant v^{(2)}_{(\min)\,n}\right) = 1 - P\left(v^{(2)}_{n} < v^{(2)}_{(\min)n}\right).$$

В результате проведенных к настоящему времени исследований с целью решения подобных задач моделирования получены аналитические выражения для показателей, аналогичных показателям вида $P(v^{(2)}_{n} \geqslant v^{(2)}_{(min)\,n})$.

В основу этих аналитических выражений положена обобщенная формула:

$$P\,(a \geqslant b) = 1 - P\,(b > a) = 1 - \int_0^{\bar{a}} f_{(b)}\,(x)\,dx, \quad (6)$$

где $f_{(b)}$ — плотность распределения случайной величины b.

Применительно к решаемой задаче входящую в выражение (6) случайную величину a можно представить в виде: $a = v^{(2)}_{n} = v^{(1)}_{n\,1} \circ v^{(1)}_{n\,2} \circ \ldots \circ v^{(1)}_{n\,\mathrm{c}} \circ \ldots \circ v^{(1)}_{n\,\mathrm{C}}$,

где $v^{(1)}_{n\,\mathrm{c}}$ — объем рабочей среды программных средств, реализующих c-ю функцию противодействия угрозам безопасности;

C — число функций, составляющих n-ый этап;

$\circ$ — операция композиции случайных величин, а случайную величину b интерпретировать как минимально допустимую величину $v^{(2)}_{(\min)\,n}$, объема рабочей среды программных средств, реализующих функции защиты информации в рамках конкретного n-го этапа возможных противоправных действий.

В результате проведенных к настоящему времени исследований с целью формирования аналитических выражений на основе (6) случайная величина $\bar{a}$ представляется в виде:

$$\bar{a} = \alpha \circ \beta = \int_0^{\infty} y \int_0^{\infty} f_{(\alpha)}(y - z)\, f_{(\beta)}\,(z)\,dz\,dy, \quad (7)$$

где $f_{(\alpha)}$, $f_{(\beta)}$ — плотности распределений случайных величин α и β.

Вероятности $P\,(a \geqslant b) = 1 - P\,(b > a)$ достаточно полно характеризуют возможности по защите информационных ресурсов компьютерных систем, связанные с реализацией этапов противодействия возможному несанкционированному доступу, копированию, модификации или уничтожению информации этих систем. Указанные вероятности использованы в диссертационной работе Александрова В. В. «Математические модели комплексной защиты информационных ресурсов органов государственного управления» в качестве промежуточных показателей второго уровня синтезируемой структуры показателей эффективности мероприятий по комплексной защите информационных ресурсов органов государственного управления.

Литература

1. *Александров В. В.* Показатели эффективности реализации информационных процессов в ИТКС в условиях противодействия угрозам информационной безопасности // Международная научно-практическая конференция «Теория и практика инновационного развития кооперативного образования и науки». Белгород, 2010. С. 18–20.
2. *Вентцель Е. С.* Теория вероятностей / М.: Изд-во физико-математической литературы, 1958. 464 с.
3. *Вентцель Е. С.* Исследование операций / М.: Советское радио, 1972. 552 с.
4. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / Под ред. С. В. Скрыля. Воронеж: Воронежский институт МВД России, 2010. 217 с.

Александров Виталий Витальевич. ст. преподаватель Белгородского университета кооперации, экономики и права. К. т. н. Кол-во печатных работ: 17 Область научных интересов: обеспечение информационной безопасности объектов. E-mail: kaf-otzi@bukep.ru

Котельников Алексей Павлович. Зав. кафедрой Белгородского университета кооперации, экономики и права. К. т. н., доцент. Окончил в 1976 г. Харьковский политехнический институт. Кол-во печатных работ: 49. Область научных интересов: математическое моделирование. E-mail: apk1703@gmail.com