УДК 004.056.53

МАТЕМАТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЬЮТЕРНЫХ СИСТЕМ

С.В. СКРЫЛЬ, А.В. МОЗГОВОЙ ДОБРЫЧЕНКО

МГТУ им. Н.Э. Баумана, Москва

e-mail: runc.nsd@gmail.com

Рассматривается методический подход к формированию математических моделей для определения временных характеристик противоправных действий в отношении информационных ресурсов компьютерных систем с целью обоснования требований к способам и средствам защиты информации от несанкционированного доступа. Приводится вариант логико-лингвистического представления функционального описания такого рода действий как инструмента их первичной формализации.

Ключевые слова: защита информации, средства защиты информации, несанкционированный доступ, математическое моделирование.

MATHEMATICAL REPRESENTATION OF ILLEGAL ACTIONS ON INFORMATION RESOURCES OF COMPUTER SYSTEMS

S.V. SKRYL, A.V. MOZGOVOY

BMSTU, Moscow

e-mail: runc.nsd@gmail.com

The paper studies the methodical approach to building mathematical models to determine the timing of illegal actions on information resources of computer systems in order to substantiate requirements to methods and facilities of protecting information from unauthorized access. In a paper has been adduced a version of the logical-linguistic representation of functional description of such activities as a tool of their primary formalization.

Keywords: information security, data protection facilities, unauthorized access, mathematical modeling.

Адекватность моделирования угроз информационной безопасности компьютерных систем является условием корректного обоснования требований к применяемым способам и средствам защиты информации от несанкционированного доступа в этих системах.

Использование методологии функционального моделирования [1] как инструмента первичной формализации информационных процессов и процессов обеспечения защиты информации сопряжено с рядом трудностей, связанных со сложностью представления такого рода процессов в рамках традиционного для данной методологии формата – графических схем (функциональных диаграмм) [2]. Следствием этого являются многочисленные ошибки

при структурировании функционального описания исследуемых процессов. Альтернативой такому подходу может рассматриваться подход, основанный на логико-лингвистическом представлении основных атрибутов функционального описания исследуемых процессов – входных и управляющих воздействий, результатов реализации описываемых функций, а так же взаимосвязей между ними. Ниже приводится вариант структуризации противоправных действий в отношении информационных ресурсов компьютерных систем как источника угроз их информационной безопасности в терминах логико-лингвистического представления исследуемого процесса. В соответствии с рассматриваемым подходом целевая функция «Реализация угроз информационной безопасности компьютерной системе (КС)» представляется в виде:

$$<\Phi^{(u)}, X^{(u)}, C^{(u)}, Y^{(u)}>,$$

где $\Phi^{(u)}$ – идентификатор целевой функции «Реализация угроз информационной безопасности КС»;

$X^{(u)}$ – идентификатор входного воздействия «Информационный процесс»;

$C^{(u)}$ – идентификатор управляющего воздействия «Воздействие угрозы информационной безопасности»;

$Y^{(u)}$ – идентификатор результата реализации функции $\Phi^{(u)}$ – «Нарушенный по условиям безопасности информационный процесс в КС».

Содержание целевой функции состоит в описании влияния угроз информационной безопасности на реализуемость информационного процесса.

Первый уровень детализации целевой функции (ее структуризации)

представляется выражением:

$$\Phi^{(u)} = <\{\phi_1^{(1)}, , c_1^{(1)}, y_1^{(1)}\} \text{ AND } (\{\phi_2^{(1)}, x_2^{(1)}, c_2^{(1)}, y_2^{(1)}\} \text{ OR } (\{\phi_3^{(1)}, x_3^{(1)}, c_3^{(1)}, y_3^{(1)}\} \text{ AND } \{\phi_2^{(1)}, x_2^{(1)}, c_2^{(1)}, y_2^{(1)}\})) \text{ AND } \{\phi_4^{(1)}, x_4^{(1)}, c_4^{(1)}, y_4^{(1)}\} \text{ AND } (\{\phi_6^{(1)}, x_6^{(1)}, c_6^{(1)}, y_6^{(1)}\} \text{OR } (\{\phi_5^{(1)}, x_5^{(1)}, c_5^{(1)}, y_5^{(1)}\} \text{ AND } \{\phi_6^{(1)}, x_6^{(1)}, c_6^{(1)}, y_6^{(1)}\}))>,$$

где $\phi_1^{(1)}$ – идентификатор функции «Физический доступ к сегменту КС»;

$c_1^{(1)}$ – идентификатор управляющего воздействия «Действия злоумышленника по организации физического доступа к КС»;

$y_1^{(1)}$ – идентификатор реализации функции $\phi_1^{(1)}$ - «Физический доступ к сегменту КС»;

$\phi_2^{(1)}$ – идентификатор функции «Вскрытие механизмов защиты информации»;

$x_2^{(1)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_2^{(1)}$ – идентификатор управляющего воздействия «Действия злоумышленника по организации вскрытия механизмов защиты»;

$y_2^{(1)}$ – идентификатор реализации функции $\phi_2^{(1)}$ - «Вскрытие механизмов защиты информации»;

$\phi_3^{(1)}$ – идентификатор функции «Внедрение ложного доверенного субъекта»;

$x_3^{(1)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_3^{(1)}$ – идентификатор управляющего воздействия «Действия злоумышленника по внедрению ложного доверенного субъекта»;

$y_3^{(1)}$ – идентификатор реализации функции $\phi_3^{(1)}$ - «Внедрение ложного доверенного субъекта»;

$\phi_4^{(1)}$ – идентификатор функции «Контроль реализации информационного процесса»;

$x_4^{(1)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_4^{(1)}$ – идентификатор управляющего воздействия «Действия злоумышленника по организации контроля реализации информационного процесса»;

$y_4^{(1)}$ – идентификатор реализации функции $\phi_4^{(1)}$ - «Контроль реализации информационного процесса»;

$\phi_5^{(1)}$ – идентификатор функции «Несанкционированное воздействие на информацию»;

$x_5^{(1)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_5^{(1)}$ – идентификатор управляющего воздействия «Вредоносное воздействие на информационный процесс в КС»;

$y_5^{(1)}$ – идентификатор реализации функции $\phi_5^{(1)}$ - «Несанкционированное воздействие на информацию»;

$\phi_6^{(1)}$ – идентификатор функции «Создание условий для последующего легального доступа»;

$x_6^{(1)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_6^{(1)}$ – идентификатор управляющего воздействия «Действия по созданию условий для последующего легального доступа к информации в КС»;

$y_6^{(1)}$ – идентификатор реализации функции $\phi_6^{(1)}$ - «Создание условий для последующего легального доступа».

Каждый из перечисленных этапов реализации угроз нарушения состояний защищенности информационного процесса представляется совокупностью процедур.

Например, функция $\Phi_3^{(1)}$, соответствующая этапу внедрения ложного доверенного субъекта, описывается следующим образом:

$$\Phi_3^{(1)} = \{\phi_{31}^{(2)}, x_{31}^{(2)}, c_{31}^{(2)}, y_{31}^{(2)}\} \text{ OR } \{\phi_{32}^{(2)}, x_{32}^{(2)}, c_{32}^{(2)}, y_{32}^{(2)}\},$$

где $\phi_{31}^{(2)}$ – идентификатор функции «Использование недостатков алгоритмов удаленного поиска»;

$x_{31}^{(2)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{31}^{(2)}$ – идентификатор управляющего воздействия «Действия злоумышленника по использованию недостатков алгоритмов удаленного поиска»;

$y_{31}^{(2)}$ – идентификатор реализации функции $\phi_{31}^{(2)}$ - «Использование недостатков алгоритмов удаленного поиска»;

$\phi_{32}^{(2)}$ – идентификатор функции «Использование недостатков в реализации сетевого сервиса»;

$x_{32}^{(2)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{32}^{(2)}$ – идентификатор управляющего воздействия «Действия злоумышленника по использованию недостатков в реализации сетевого сервиса»;

$y_{32}^{(2)}$ – идентификатор реализации функции $\phi_{32}^{(2)}$ - «Использование не-

достатков в реализации сетевого сервиса».

Каждая функция второго уровня декомпозиции исследуемого процесса (структуризации целевой функции) представляется совокупностью функций третьего уровня.

Например, функция $\phi_{32}^{(2)}$ использования недостатков алгоритмов удаленного поиска описывается следующим образом:

$$\Phi_{32}^{(2)} = \{\phi_{321}^{(3)}, x_{321}^{(3)}, c_{321}^{(3)}, y_{321}^{(3)}\} \text{ OR } \{\phi_{322}^{(3)}, x_{322}^{(3)}, c_{322}^{(3)}, y_{322}^{3)}\},$$

где $\phi_{321}^{(3)}$ – идентификатор функции «Навязывание хосту ложного маршрута с использованием протокола ICMP»;

$x_{321}^{(3)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{321}^{(3)}$ – идентификатор управляющего воздействия «Действия по навязыванию хосту ложного маршрута с использованием протокола ICMP»;

$y_{321}^{(3)}$ – идентификатор реализации функции $\phi_{321}^{(3)}$ - «Навязывание хосту ложного маршрута с использованием протокола ICMP»;

$\phi_{322}^{(3)}$ – идентификатор функции «Использование других недостатков сетевого сервиса»;

$x_{322}^{(3)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{322}^{(3)}$ – идентификатор управляющего воздействия «Действия по использованию других недостатков сетевого сервиса»;

$y_{322}^{(3)}$ – идентификатор реализации функции $\phi_{322}^{(3)}$ - «Использование других недостатков сетевого сервиса».

Каждая из функций третьего уровня декомпозиции функциональной модели противоправных действий по реализации угроз информационной безопасности КС представляется функциями четвертого уровня.

Например, функция $\phi_{322}^{(3)}$ использования недостатков сетевого сервиса описывается следующим образом:

$$\Phi_{322}^{(3)} = \{\phi_{3221}^{(4)}, x_{3221}^{(4)}, c_{3221}^{(4)}, y_{3221}^{(4)}\} \text{ OR } \{\phi_{3222}^{(4)}, x_{3222}^{(4)}, c_{3222}^{(4)}, y_{3222}^{(4)}\},$$

где $\phi_{3221}^{(4)}$ – идентификатор функции «Подмена абонента в TCP-соединении»;

$x_{3221}^{(4)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{3221}^{(4)}$ – идентификатор управляющего воздействия «Действия по осуществлению атаки путем подмены абонента в TCP-соединении»;

$y_{3221}^{(4)}$ – идентификатор реализации функции $\phi_{3221}^{(4)}$ - «Подмена абонента в TCP-соединении»;

$\phi_{3222}^{(4)}$ – идентификатор функции «Ошибки реализации сетевых служб»;

$x_{3222}^{(4)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{3222}^{(4)}$ – идентификатор управляющего воздействия «Действия по осуществлению атаки путем навязывания ошибок реализации сетевых служб»;

$y_{3222}^{(4)}$ – идентификатор реализации функции $\phi_{3222}^{(4)}$ - «Ошибки реализа-

ции сетевых служб».

Каждая из функций четвертого уровня декомпозиции исследуемого процесса (структуризации целевой функции) представляется совокупностью функций пятого уровня.

Например, функция $\phi_{3221}^{(4)}$ подмены абонента в TCP-соединении описывается следующим образом:

$$\Phi_{3221}^{(4)} = \{\phi_{32211}^{(5)}, x_{32211}^{(5)}, c_{32211}^{(5)}, y_{32211}^{(5)}\} \text{ OR } \{\phi_{32212}^{(5)}, x_{32212}^{(5)}, c_{32212}^{(5)}, y_{32212}^{(5)}\} \text{ OR } \{\phi_{32213}^{(5)}, x_{32213}^{(5)}, c_{32213}^{(5)}, y_{32213}^{(5)}\},$$

где $\phi_{32211}^{(5)}$ – идентификатор функции «Подмена анализом значения идентификатора соединения»;

$x_{32211}^{(5)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{32211}^{(5)}$ – идентификатор управляющего воздействия «Действия по осуществлению атаки путем подмены анализом значения идентификатора соединения»;

$y_{32211}^{(5)}$ – идентификатор реализации функции $\phi_{32211}^{(5)}$ - «Подмена анализом значения идентификатора соединения»;

$\phi_{32212}^{(5)}$ – идентификатор функции «Шторм ложных запросов», направленных на сервер»;

$x_{32212}^{(5)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{32212}^{(5)}$ – идентификатор управляющего воздействия «Действия по осуществлению атаки путем осуществления «шторма ложных за-

просов», направленных на сервер»;

$y_{32212}^{(5)}$ – идентификатор реализации функции $\phi_{32212}^{(5)}$ - «Шторм ложных запросов», направленных на сервер»;

$\phi_{32213}^{(5)}$ – идентификатор функции «Шторм ложных запросов», направленных на объект воздействия»;

$x_{32213}^{(5)}$ – идентификатор входного воздействия «Информационный процесс»;

$c_{32213}^{(5)}$ – идентификатор управляющего воздействия «Действия по осуществлению атаки путем осуществления «шторма ложных запросов», направленных на объект воздействия»;

$y_{32213}^{(5)}$ – идентификатор реализации функции $\phi_{32213}^{(5)}$ - «Шторм ложных запросов», направленных на объект воздействия».

Пятиуровневая детализация целевой функции «Реализация угроз информационной безопасности компьютерной системе» является приемлемой для использования результатов структуризации для формализации противоправных действий в отношении информационных ресурсов компьютерных систем.

Представим временную характеристику произвольной *i*-й функции 5-го уровня рассматриваемой функциональной модели в виде:

$$T_i = <\tau_i, \sigma_i, min_i, max_i>,$$

где *i* – порядковый номер функции, полученный в результате преобразования ее индекса и уровня;

τ_i, - среднее значение случайной величины времени выполнения i-й функции;

σ_i – ее среднеквадратическое значение;

min_i, max_i – соответственно, минимальное и максимальное значения данной случайной величины.

С учетом 5-значной индексации *klmns* функций 5-го уровня функциональной модели противоправных действий в отношении информационных ресурсов компьютерных систем порядковый номер функции i определяется в соответствии с выражением:

$$i = C_1 + C_2 + C_3 + C_4 + C_5 + s,$$

в котором $C_1 = \begin{cases} \sum_{a=1}^{k-1} \sum_{b=1}^{c_a^1} \sum_{d=1}^{c_{ab}^2} \sum_{e=1}^{c_{abd}^3} \sum_{f=1}^{c_{abde}^4} c_{abdef}^5, \; при \; k > 1; \\ 0, \; при \; k = 1, \end{cases}$,

$C_2 = \begin{cases} \sum_{b=1}^{l-1} \sum_{d=1}^{c_{ab}^2} \sum_{e=1}^{c_{abd}^3} \sum_{f=1}^{c_{abde}^4} c_{abdef}^5, \; при \; l > 1; \\ 0, \; при \; l = 1, \end{cases}$

$C_3 = \begin{cases} \sum_{d=1}^{m-1} \sum_{e=1}^{c_{abd}^3} \sum_{f=1}^{c_{abde}^4} c_{abdef}^5, \; при \; m > 1; \\ 0, \; при \; m = 1, \end{cases}$

$C_4 = \begin{cases} \sum_{e=1}^{n-1} \sum_{f=1}^{c_{abde}^4} c_{abdef}^5, \; при \; n > 1; \\ 0, \; при \; n = 1, \end{cases}$

$$C_5 = \begin{cases} \sum_{f=1}^{s-1} c^5_{abdef}, \text{ при } s > 1; \\ 0, \text{ при } s = 1, \end{cases}$$

где $c_a^{(1)}$ - количество функций второго уровня функциональной модели *a*-ой функции первого уровня;

$c_{ab}^{(2)}$ - количество функций третьего уровня функциональной модели *b*-ой функции второго уровня;

$c_{abd}^{(3)}$ - количество функций четвертого уровня функциональной модели *d*-ой функции 3-го уровня;

$c_{abde}^{(4)}$ - количество функций пятого уровня функциональной модели *e*-ой функции 4-го уровня;

$c_{abdef}^{(5)}$ - порядковый номер функции пятого уровня *e*-ой функции 4-го уровня.

В соответствии с функциональным представлением противоправных действий в отношении информационных ресурсов компьютерных систем возможен последовательный (функциональная связь AND) и параллельный (функциональная связь OR) порядок реализации функций.

Последовательная реализация порядка выполнения функций соответствующих уровней рассмотренной функциональной модели математически представляется в виде композиций двух, трех и четырех случайных величин. В соответствии с [3] среднее значение времени τ реализации функций в таких последовательностях определяется в соответствии с выражениями:

для двух случайных величин:

$$\overline{\tau} = M\left(\tau_{\mathrm{I}} \circ \tau_{\mathrm{II}}\right) = \int_{\tau_{\min \mathrm{I}}}^{\infty} u \int_{\tau_{\min \mathrm{II}}}^{\infty} f_{\mathrm{I}}(u-v)\, f_{\mathrm{II}}(v)\, dv\, du , \quad (1)$$

где f_{I} и f_{II} – плотности распределений случайных величин времени τ_{I} и τ_{II}, реализации функций в их последовательности;

$\tau_{min\mathrm{I}}$ и $\tau_{min\mathrm{II}}$ – минимальные значения этих величин;

$M(\cdot)$ - математическое ожидание от их композиции;

для трех случайных величин:

$$\overline{\tau} = M\left(\tau_{\mathrm{I}} \circ \tau_{\mathrm{II}} \circ \tau_{\mathrm{III}}\right) = \int_{\tau_{\min \mathrm{I}}}^{\infty} \int_{\tau_{\min \mathrm{II}}}^{u} \int_{\tau_{\min \mathrm{III}}}^{w} u \cdot f_{\mathrm{I}}(v) \cdot f_{\mathrm{II}}(w-v) \cdot f_{\mathrm{III}}(u-w)\, dv dw du , \quad (2)$$

где f_{I}, f_{II} и f_{III} – плотности распределений случайных величин времени $\tau_{\mathrm{I}}, \tau_{\mathrm{II}}$ и τ_{III} реализации функций в их последовательности;

$\tau_{min\mathrm{I}}, \tau_{min\mathrm{II}}$ и $\tau_{min\mathrm{III}}$ – минимальные значения этих величин;

для четырех случайных величин:

$$\overline{\tau} = M\left(\tau_{\mathrm{I}} \circ \tau_{\mathrm{II}} \circ \tau_{\mathrm{III}} \circ \tau_{\mathrm{IV}}\right) = \int_{\tau_{\min \mathrm{I}}}^{\infty} \int_{\tau_{\min \mathrm{II}}}^{u} \int_{\tau_{\min \mathrm{III}}}^{w} \int_{\tau_{\min \mathrm{IV}}}^{z} u \cdot f_1(u_{\mathrm{I}}) \cdot f_2(u_{\mathrm{II}} - v) \cdot f_3(z-w) \cdot f_4(u-z)\, dv\, dw dz du , \quad (3)$$

где f_{I}, f_{II}, f_{III} и f_{VI} – плотности распределений случайных величин времени $\tau_{\mathrm{I}}, \tau_{\mathrm{II}}, \tau_{\mathrm{III}}$ и τ_{IV} реализации функций в их последовательности;

$\tau_{min\mathrm{I}}, \tau_{min\mathrm{II}}, \tau_{min\mathrm{III}}$ и $\tau_{min\mathrm{IV}}$ – минимальные значения этих величин.

Среднее значение времени τ реализации функций противоправных действий в отношении информационных ресурсов компьютерных систем в случае

параллельного порядка их выполнения на соответствующих уровнях функциональной модели такого рода действий математически представляется в виде:

$$\overline{\tau} = p_{\text{I}} \cdot \overline{\tau}_{\text{I}} + p_{\text{II}} \cdot \overline{\tau}_{\text{II}} + \ldots + p_N \cdot \overline{\tau}_N , \qquad (4)$$

где p_{I}, p_{II}, … , p_N – вероятность выполнения соответствующей функции.

В общем случае, в соответствии с функциональным представлением противоправных действий в отношении информационных ресурсов компьютерных систем возможны варианты последовательного и параллельного порядка реализации функций. В этом случае для определения среднего значения времени τ реализации функций подобного рода действий используются выражения (1) – (4) для соответствующих фрагментов порядка реализации этих функций.

При получении среднего значения времени τ реализации функций противоправных действий в отношении информационных ресурсов компьютерных систем на любом из уровней функциональной модели такого рода действий (за исключением пятого) в качестве исходных данных используются временные характеристики функций предыдущего уровня. При этом, данные по временным характеристикам пятого уровня функциональной модели задаются. Для представления исходных данных третьего, второго и первого уровней функциональной модели временные характеристики функций четвертого, третьего и второго уровней, соответственно, определяются в соответствии с критерием Колмогорова – Смирнова [4].

СПИСОК ЛИТЕРАТУРЫ

1. Калянов Г.Н. CASE: Структурный системный анализ (автоматизация и применение). - М.: Лори, 1996. - 242 с.

2. Функциональное моделирование как методология исследования информационной деятельности / С.В. Скрыль, А.А. Малышев, С.Н. Волкова, А.А. Герасимов // Интеллектуальные системы (INTELS’ 2010): Труды Девятого международного симпозиума. – М.: РУСАКИ, 2010. – С. 590 – 593.

3. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / под ред. С.В. Скрыля – Воронеж: Воронежский институт МВД России, 2010. – 217 с.

4. Вентцель Е.С. Теория вероятностей. — М.: Изд-во физико-математической литературы, 1958. — 464 с.

REFERENCES

1. Kalyanov G.N. CASE: Structured System Analysis (automation and application). - M: Lori, 1996. - 242 p.
2. Functional modeling as a methodology for the research of information activities / S.V. Skryl, A.A. Malyshev, S.N. Volkova, A.A. Gerasimov / / Intelligent Systems (INTELS '2010): Proceedings of the Ninth International Symposium. - M. RUSAKI, 2010. - P. 590 - 593.
3. Security evaluation of information processes in the territorial departments of Internal Affairs: research models: monograph / ed. S.V. Skryl - Voronezh: Voronezh Institute of Russian Ministry of Internal Affairs, 2010. - 217 p.
4. Wentzel E.S. Probability. - Moscow: Publishing House of Physical and Mathematical Literature, 1958. - 464.