УДК 004.056.53

Математическое представление противоправных действий в отношении информационных ресурсов компьютерных систем

© С.В. Скрыль, А.В. Мозговой, А.И. Добрыченко

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрен 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. Приведен 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.*

Адекватность моделирования угроз информационной безопасности компьютерных систем (КС) является необходимым условием для 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. В качестве альтернативы такому подходу предлагается подход, основанный на логико-лингвистическом представлении основных атрибутов функционального описания исследуемых процессов — входных и управляющих воздействий, результатов реализации описываемых функций, а также взаимосвязей между ними.

Далее 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 «Реали-

зация угроз информационной безопасности компьютерной системы» представляется в виде

$$\left\langle \Phi^{(\text{ц})},\ X^{(\text{ц})}, C^{(\text{ц})},\ Y^{(\text{ц})} \right\rangle,$$

где $\Phi^{(\text{ц})}$ — идентификатор целевой функции «Реализация угроз информационной безопасности КС»; $X^{(\text{ц})}$ — идентификатор входного воздействия «Информационный процесс»; $C^{(\text{ц})}$ — идентификатор управляющего воздействия «Воздействие угрозы информационной безопасности»; $Y^{(\text{ц})}$ — идентификатор результата реализации функции $\Phi^{(\text{ц})}$ «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

$$\begin{aligned}\Phi^{(\text{ц})} = \Big\langle \Big\{ \phi_1^{(1)},\ \ , c_1^{(1)}, y_1^{(1)} \Big\} \text{AND} \Big(\Big\{ \phi_2^{(1)}, x_2^{(1)}, c_2^{(1)}, y_2^{(1)} \Big\} \\ \text{OR} \Big(\Big\{ \phi_3^{(1)}, x_3^{(1)}, c_3^{(1)}, y_3^{(1)} \Big\} \text{AND} \Big\{ \phi_2^{(1)}, x_2^{(1)}, c_2^{(1)}, y_2^{(1)} \Big\} \Big) \Big) \\ \text{AND} \Big\{ \phi_4^{(1)}, x_4^{(1)}, c_4^{(1)}, y_4^{(1)} \Big\} \text{AND} \Big(\Big\{ \phi_6^{(1)}, x_6^{(1)}, c_6^{(1)}, y_6^{(1)} \Big\} \\ \text{OR} \Big(\Big\{ \phi_5^{(1)}, x_5^{(1)}, c_5^{(1)}, y_5^{(1)} \Big\} \text{AND} \Big\{ \phi_6^{(1)}, x_6^{(1)}, c_6^{(1)}, y_6^{(1)} \Big\} \Big) \Big) \Big\rangle,\end{aligned}$$

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 $\phi_1^{(1)}$; $\phi_2^{(1)}$ — идентификатор функции «Вскрытие механизмов защиты информации»; $x_2^{(1)}$, $x_3^{(1)}$, $x_4^{(1)}$, $x_5^{(1)}$, $x_6^{(1)}$ — идентификаторы входного воздействия «Информационный процесс»; $c_2^{(1)}$ — идентификатор управляющего воздействия «Действия злоумышленника по организации вскрытия механизмов защиты»; $\phi_3^{(1)}$ — идентификатор функции «Внедрение ложного доверенного субъекта»; $c_3^{(1)}$ — идентификатор управляющего воздействия «Действия злоумышленника по внедрению ложного доверенного субъекта»; $\phi_4^{(1)}$ — идентификатор функции «Контроль ре-

ализации информационного процесса»; $c_4^{(1)}$ — идентификатор управляющего воздействия «Действия злоумышленника по организации контроля реализации информационного процесса»; $\phi_5^{(1)}$ — идентификатор функции «Несанкционированное воздействие на информацию»; $c_5^{(1)}$ — идентификатор управляющего воздействия «Вредоносное воздействие на информационный процесс в КС»; $\phi_6^{(1)}$ — идентификатор функции «Создание условий для последующего легального доступа»; $c_6^{(1)}$ — идентификатор управляющего воздействия «Действия по созданию условий для последующего легального доступа к информации в КС»; $y_2^{(1)}$, $y_3^{(1)}$, $y_4^{(1)}$, $y_5^{(1)}$, $y_6^{(1)}$ — идентификаторы реализации функций $\phi_2^{(1)}$, $\phi_3^{(1)}$, $\phi_4^{(1)}$, $\phi_5^{(1)}$, $\phi_6^{(1)}$ соответственно.

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:

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

где $\phi_{31}^{(2)}$ — идентификатор функции «Использование недостатков алгоритмов удаленного поиска»; $x_{31}^{(2)}$, $x_{32}^{(2)}$ — идентификаторы входного воздействия «Информационный процесс»; $c_{31}^{(2)}$ — идентификатор управляющего воздействия «Действия злоумышленника по использованию недостатков алгоритмов удаленного поиска»; $\phi_{32}^{(2)}$ — идентификатор функции «Использование недостатков в реализации сетевого сервиса»; $c_{32}^{(2)}$ — идентификатор управляющего воздействия «Действия злоумышленника по использованию недостатков в реализации сетевого сервиса»; $y_{31}^{(2)}$, $y_{32}^{(2)}$ — идентификаторы реализации функций $\phi_{31}^{(2)}$, $\phi_{32}^{(2)}$ соответственно.

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

Например, функция $\Phi_{32}^{(2)}$ использования недостатков в реализации сетевого сервиса описывается следующим образом:

$$\Phi_{32}^{(2)} = \left\{\phi_{321}^{(3)}, x_{321}^{(3)}, c_{321}^{(3)}, y_{321}^{(3)}\right\} \mathrm{OR} \left\{\phi_{322}^{(3)}, x_{322}^{(3)}, c_{322}^{(3)}, y_{332}^{(3)}\right\},$$

где $\phi_{321}^{(3)}$ — идентификатор функции «Навязывание хосту ложного маршрута с использованием протокола ICMP»; $x_{321}^{(3)}$, $x_{322}^{(3)}$ — идентификаторы входного воздействия «Информационный процесс»; $c_{321}^{(3)}$ — идентификатор управляющего воздействия «Действия по навязыванию хосту ложного маршрута с использованием протокола ICMP»; $\phi_{322}^{(3)}$ — идентификатор функции «Использование других недостатков сетевого сервиса»; $c_{322}^{(3)}$ — идентификатор управляющего воздействия «Действия по использованию других недостатков сетевого сервиса»; $y_{321}^{(3)}$, $y_{322}^{(3)}$ — идентификаторы реализации функций $\phi_{321}^{(3)}$, $\phi_{322}^{(3)}$ соответственно.

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

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

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

где $\phi_{3221}^{(4)}$ — идентификатор функции «Подмена абонента в TCP-соединении»; $x_{3221}^{(4)}$, $x_{3222}^{(4)}$ — идентификаторы входного воздействия «Информационный процесс»; $c_{3221}^{(4)}$ — идентификатор управляющего воздействия «Действия по осуществлению атаки путем подмены абонента в TCP-соединении»; $\phi_{3222}^{(4)}$ — идентификатор функции «Ошибки реализации сетевых служб»; $c_{3222}^{(4)}$ — идентификатор управляющего воздействия «Действия по осуществлению атаки путем навязывания ошибок реализации сетевых служб»; $y_{3221}^{(4)}$, $y_{3222}^{(4)}$ — идентификаторы реализации функций $\phi_{3221}^{(4)}$, $\phi_{3222}^{(4)}$ соответственно.

Каждая функция 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:

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

где $\phi_{32211}^{(5)}$ — идентификатор функции «Подмена абонента с помощью анализа значения идентификатора соединения»; $x_{32211}^{(5)}$, $x_{32212}^{(5)}$, $x_{32213}^{(5)}$ —

идентификаторы входного воздействия «Информационный процесс»; $c_{32211}^{(5)}$ — идентификатор управляющего воздействия «Действия по осуществлению атаки путем подмены абонента с помощью анализа значения идентификатора соединения»; $\phi_{32212}^{(5)}$ — идентификатор функции «“Шторм ложных запросов”, направленных на сервер»; $c_{32212}^{(5)}$ — идентификатор управляющего воздействия «Действия по реализации атаки путем осуществления “шторма ложных запросов”, направленных на сервер»; $\phi_{32213}^{(5)}$ — идентификатор функции «“Шторм ложных запросов”, направленных на объект воздействия»; $c_{32213}^{(5)}$ — идентификатор управляющего воздействия «Действия по реализации атаки путем осуществления “шторма ложных запросов”, направленных на объект воздействия»; $y_{32211}^{(5)}$, $y_{32212}^{(5)}$, $y_{32213}^{(5)}$ — идентификаторы реализации функций $\phi_{32211}^{(5)}$, $\phi_{32212}^{(5)}$, $\phi_{32213}^{(5)}$ соответственно.

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

Представим временну́ю характеристику произвольной i-й функции пятого уровня рассматриваемой функциональной модели в виде

$$T_i = \langle \tau_i, \sigma_i, \min_i, \max_i \rangle,$$

где i — порядковый номер функции, полученный в результате преобразования ее индекса и уровня; τ_i и σ_i — соответственно среднее и среднеарифметическое значения случайной величины времени выполнения i-й функции; $\min_i$, $\max_i$ — соответственно минимальное и максимальное значения данной случайной величины.

С учетом пятизначной индексации $klmns$ функций пятого уровня функциональной модели противоправных действий в отношении информационных ресурсов компьютерных систем порядковый номер i функции определяется в соответствии с выражением

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

в котором

$$C_1 = \begin{cases} \sum\limits_{a=1}^{k-1} \sum\limits_{b=1}^{c_a^{(1)}} \sum\limits_{d=1}^{c_{ab}^{(2)}} \sum\limits_{e=1}^{c_{abd}^{(3)}} \sum\limits_{f=1}^{c_{abde}^{(4)}} c_{abdef}^{(5)} & \text{при } k > 1, \\ 0 & \text{при } k = 1; \end{cases}$$

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

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

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

$$C_5 = \begin{cases} \sum_{f=1}^{s-1} c_{abdef}^{(5)} & \text{при } s > 1, \\ 0 & \text{при } s = 1, \end{cases}$$

где $c_a^{(1)}$ — количество функций второго уровня функциональной модели a-й функции первого уровня; $c_{ab}^{(2)}$ — количество функций третьего уровня функциональной модели b-й функции второго уровня; $c_{abd}^{(3)}$ — количество функций четвертого уровня функциональной модели d-й функции третьего уровня; $c_{abde}^{(4)}$ — количество функций пятого уровня функциональной модели e-й функции четвертого уровня; $c_{abdef}^{(5)}$ — порядковый номер функции пятого уровня e-й функции четвертого уровня.

В соответствии с функциональным представлением противоправных действий в отношении информационных ресурсов КС возможен как последовательный (функциональная связь AND), так и параллельный (функциональная связь OR) порядок выполнения функций.

Последовательную реализацию функций соответствующих уровней рассмотренной функциональной модели математически можно представить в виде композиций двух, трех и четырех случайных величин. В соответствии с [3] среднее значение времени τ реализации функций в таких последовательностях определяется следующими выражениями:

• для двух случайных величин u и v

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

• для трех случайных величин u, v и w

$$\overline{\tau} = M\left(\tau_{\mathrm{I}} \circ \tau_{\mathrm{II}} \circ \tau_{\mathrm{III}}\right) =$$

$$= \int\limits_{\tau_{\min \mathrm{I}}}^{\infty} \int\limits_{\tau_{\min \mathrm{II}}}^{v} \int\limits_{\tau_{\min \mathrm{III}}}^{w} u f_{\mathrm{I}}(u) f_{\mathrm{II}}(u-v) f_{\mathrm{III}}(v-w)\, dw\, dv\, du; \qquad (2)$$

• для четырех случайных величин u, v, w и z

$$\overline{\tau} = M\left(\tau_{\mathrm{I}} \circ \tau_{\mathrm{II}} \circ \tau_{\mathrm{III}} \circ \tau_{\mathrm{IV}}\right) =$$

$$= \int\limits_{\tau_{\min \mathrm{I}}}^{\infty} \int\limits_{\tau_{\min \mathrm{II}}}^{v} \int\limits_{\tau_{\min \mathrm{III}}}^{w} \int\limits_{\tau_{\min \mathrm{IV}}}^{z} u f_{\mathrm{I}}(u) f_{\mathrm{II}}(u-v) f_{\mathrm{III}}(v-w) f_{\mathrm{IV}}(w-z)\, dz\, dw\, dv\, du, \qquad (3)$$

где f_{I}, f_{II}, f_{III} и f_{IV} — плотности распределений случайных величин времени τ_{I}, τ_{II}, τ_{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; $M(\cdot)$ — математическое ожидание их композиции.

Среднее значение времени τ реализации функций противоправных действий в отношении информационных ресурсов КС в случае *параллельного порядка* их выполнения на соответствующих уровнях функциональной модели такого рода действий математически представляется в виде

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

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

В общем случае, согласно функциональному представлению противоправных действий в отношении информационных ресурсов КС, возможны различные варианты чередования последовательного и параллельного порядков реализации функций. 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 КС на любом из уровней функциональной модели такого рода действий (за исключением пятого) в качестве исходных данных используются временные характеристики функций предыдущего уров-

ня. При этом временные характеристики 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 согласно критерию Колмогорова – Смирнова [4].

ЛИТЕРАТУРА

[1] Калянов Г.Н. *CASE: Структурный системный анализ (автоматизация и применение)*. Москва, Лори, 1996, 242 с.

[2] Скрыль С.В., Малышев А.А., Волкова С.Н., Герасимов А.А. Функциональное моделирование как методология исследования информационной деятельности. *Интеллектуальные системы (INTELS' 2010): Тр. 9-го Междунар. симп.* Москва, РУСАКИ, 2010, с. 590–593.

[3] Скрыль С.В., ред. *Оценка защищенности информационных процессов в территориальных ОВД: модели исследования*. Воронежский институт МВД России, 2010, 217 с.

[4] Вентцель Е.С. *Теория вероятностей*. Москва, Изд-во физ.-мат. лит., 1958, 464 с.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Скрыль С.В., Мозговой А.В., Добрыченко А.И. Математическое представление противоправных действий в отношении информационных ресурсов компьютерных систем. *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/1022.html

Скрыль Сергей Васильевич – д-р техн. наук, профессор кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 100 научных работ, 7 авторских свидетельств, 15 учебно-методических работ по тематике «Защита информации».

Мозговой Андрей Валериевич родился 1986 г., окончил МГТУ им. Н.Э. Баумана в 2009 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор более 10 статей по тематике «Защита информации». e-mail: runc.nsd@gmail.com

Добрыченко Анна Игоревна родилась в 1987 г., окончила МГТУ им. Н.Э. Баумана в 2011 г. Ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Автор одной научной статьи в области защиты государственной тайны. e-mail: drozdova-zi@mail.ru