УДК 004.942
doi: 10.21685/2072-3059-2025-3-5

Функциональная модель этапа доступа к отдельному средству вычислительной техники в процессе вирусной атаки в компьютерных системах

Р. А. Хворов[1], К. С. Скрыль[2], И. И. Корчагин[3], К. Е. Амелина[4], В. В. Гайфулин[5], И. В. Савельев[6]

[1]Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина, Воронеж, Россия
[2,4]Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет), Москва, Россия
[3]АО «Информационная внедренческая компания», Москва, Россия
[5,6]Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, Краснодар, Россия

[1]khvoroff@rambler.ru, [2]kskryl@bmstu.ru, [3]korchagin@ivk.ru, [4]amelina@bmstu.ru, [5]gayfulin2007@yandex.ru, [6]kvvu@mil.ru

Аннотация. *Актуальность и цели*. Повышение адекватности математических моделей воздействия вредоносного программного обеспечения (ВПО), используемых для обоснования требований к характеристикам и направлениям совершенствования антивирусных механизмов компьютерных систем (КС), может быть достигнуто использованием методического аппарата функционального моделирования. Цель – обоснование методического аппарата для формализации угроз воздействия ВПО с целью построения адекватных математических моделей для оценки временных характеристик такого рода угроз. *Материалы и методы.* Решение задачи построения функциональных моделей в компьютерных системах производится на основе методологии функционального моделирования, системного анализа и теории графов. *Результаты*. Обоснована и реализована процедура построения математических моделей временных характеристик угроз воздействия ВПО, включающая: этап детализации целевой функции «Воздействие ВПО», этап установления порядка выполнения ее функциональных компонент на каждом из уровней декомпозиции, этап формирования пространства признаков воздействия ВПО, этап представления модели в виде графов и этап формирования аналитических выражений для оценки временных характеристик угрозы. *Выводы*. Достигаемая за счет функциональной декомпозиции целевой функции «Воздействие ВПО» адекватность математических моделей временных характеристик угроз такого воздействия позволяет обеспечить обоснованность требований к направлениям совершенствования антивирусных механизмов КС.

Ключевые слова: функциональное моделирование, марковский процесс, вредоносное программное обеспечение, математические модели воздействия вредоносного программного обеспечения

Для цитирования: Хворов Р. А., Скрыль К. С., Корчагин И. И., Амелина К. Е., Гайфулин В. В., Савельев И. В. Функциональная модель этапа доступа к отдельному средству вычислительной техники в процессе вирусной атаки в компьютерных системах // Известия высших учебных заведений. Поволжский регион. Технические науки. 2025. № 3. С. 74–85. doi: 10.21685/2072-3059-2025-3-5

The functional model of stage access to a separate computer hardware in the process of a virus attack in computer systems

R.A. Khvorov[1], K.S. Skryl'[2], I.I. Korchagin[3], K.E. Amelina[4], V.V. Gayfulin[5], I.V. Savel'ev[6]

[1]Military Training and Scientific Center of the Air Force "Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin", Voronezh, Russia
[2,4]Bauman Moscow State Technical University (National Research University), Moscow, Russia
[3]Information Implementation Company JSC, Moscow, Russia
[5,6]Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia

[1]khvoroff@rambler.ru, [2]kskryl@bmstu.ru, [3]korchagin@ivk.ru, [4]amelina@bmstu.ru, [5]gayfulin2007@yandex.ru, [6]kvvu@mil.ru

Abstract. *Background*. Increasing the adequacy of mathematical models of the impact of malicious software (MS), used to substantiate the requirements for the characteristics and directions for improving the anti-virus mechanisms of computer systems (CS), can be achieved by using the methodological apparatus of functional modeling. The purpose of the studyis to substantiate a methodological apparatus for formalizing the threats of MS in order to construct adequate mathematical models for assessing the temporal characteristics of such threats. *Materials and methods.* The solution to the problem of constructing functional models in computer systems is based on the methodology of functional modeling, systems analysis and graph theory. *Rusults*. A procedure for constructing mathematical models of the temporal characteristics of threats of MS has been substantiated and implemented, including: a stage of detailing the objective function "Impact of MS", a stage of establishing the order of execution of its functional components at each level of decomposition, a stage of forming the space of MS features, a stage of presenting the model in the form of graphs and a stage of forming analytical expressions for assessing the temporal characteristics of the threat. *Conclusions*. The adequacy of mathematical models of the temporal characteristics of threats of such impact, achieved through the functional decomposition of the objective function "Impact of MS", allows for the validity of requirements for the directions of improvement of anti-virus mechanisms of the CS.

Keywords: functional modeling, Markov process, malicious software, mathematical models of the impact of malicious software

For citation: Khvorov R.A., Skryl' K.S., Korchagin I.I., Amelina K.E., Gayfulin V.V., Savel'ev I.V. The functional model of stage access to a separate computer hardware in the process of a virus attack in computer systems. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki = University proceedings. Volga region. Engineering sciences.* 2025;(3):74–85. (In Russ.). doi: 10.21685/2072-3059-2025-3-5

Введение

Характерной особенностью исследований в сфере информационной безопасности является отсутствие возможности проведения натурных экспериментов на функционирующих информационных системах. Это обусловлено наличием рисков неконтролируемого нарушения безопасности информации этих систем и как следствие – существенным ущербом для тех сфер деятельности, в интересах которых данные системы функционируют. Подобного рода обстоятельства приводят к безальтернативному использованию математического моделирования в качестве методологии исследования в данной

сфере. Это в свою очередь порождает довольно серьезную как в теоретическом, так и в практическом плане проблему адекватности применяемых математических моделей.

Устранение данной проблемы применительно к разработке адекватных математических моделей воздействия вредоносного программного обеспечения (ВПО) связано с тем обстоятельством, что модель подобного рода угрозы безопасности информации следует рассматривать как источник информации о ней. Это, в свою очередь позволяет, в соответствии с положениями классической теории информации [1–4], сделать вывод о том, что чем больше состояний угрозы воздействия ВПО будет представлено моделью, тем большее количество информации об угрозе будет получено путем ее моделирования, а, следовательно, такая модель будет более адекватной. С этой целью была предложена четырехэтапная процедура построения математических моделей временных характеристик процессов воздействия ВПО:

– первый этап – структуризация целевой функции «Воздействие ВПО» путем ее декомпозиции на отдельные уровни с последующим определением множества функциональных компонент на каждом уровне;

– второй этап – определение порядка реализации ее функциональных компонент;

– третий этап – формальное представление порядка реализации рассматриваемой целевой функции марковским процессом;

– четвертый этап – построение аналитических выражений для определения временных характеристик отдельных компонент и самой целевой функции «Воздействие ВПО» в целом.

Цель исследования – описать приведенную последовательность для случая построения математических моделей временных характеристик используемых тактик доступа к отдельным средствам вычислительной техники (СВТ) в процессе вирусной атаки как совокупности техник применения тех или иных вирусных механизмов.

Четырехэтапная процедура построения математических моделей временных характеристик процессов воздействия вредоносного программного обеспечения

На первом этапе путем детализации функциональной компоненты «Доступ к отдельному СВТ – объекту вирусной атаки» (этап $Э_1^{(в)}$ реализации целевой функции «Воздействие ВПО») образуются уровни ее функциональной декомпозиции: уровень тактик и уровень техник. Исходя из того, что техники применения тех или иных вирусных механизмов проявляются в операционной среде компьютерной системы (КС) в виде соответствующих признаков, обнаруживаемых и идентифицируемых как средствами контроля и диагностики операционной системы, так и антивирусными средствами, уровень техник является конечным уровнем декомпозиции целевой функции.

На втором этапе устанавливается порядок реализации (выполнения) техник в рамках тактики. При этом характер взаимосвязей между данными функциональными компонентами определяется эмпирически [5]. Формируемые таким образом функциональные модели доступа к отдельным СВТ в процессе вирусной атаки описываются терминами функциональных диаграмм.

На третьем этапе модели в терминах функциональных диаграмм представляются в виде графов, описывающих процесс доступа к отдельным СВТ – объектам вирусной атаки как марковского процесса [6].

На четвертом этапе формируются аналитические выражения для оценки временных характеристик функциональных компонент, реализуемых в процессе доступа к отдельному СВТ в результате вирусной атаки.

Дадим структурное представление первой из функциональных компонент целевой функции «Воздействие ВПО» – этапу доступа к отдельному СВТ в процессе вирусной атаки. В дальнейшем данный этап будем рассматривать как частную целевую функцию, повторив при этом для нее рассмотренную выше четырехэтапную процедуру построения математических моделей временных характеристик процессов воздействия ВПО.

На первом этапе данной процедуры исходя из динамики достижения нарушителем своей цели при реализации частной целевой функции «Доступ к отдельному СВТ в процессе вирусной атаки» нарушителю необходимо осуществить внедрение и инициировать работу вредоносной программы, обеспечить выявление ею уязвимостей базовых компонент программного обеспечения (ПО) путем анализа их работы в операционной среде КС с целью получения высокого уровня доступа в операционной среде и обхода механизма антивирусной защиты путем скрытия своей активности, а также обеспечить постоянный доступ к операционной среде КС путем ассоциирования с программами автозагрузки и связь с контрольным сервером для управления процессами в операционной среде и сбора необходимых данных для доступа к отдельным СВТ в КС [7].

Воспользовавшись терминологий базового документа ФСТЭК [8], регламентирующего порядок проведения исследований с целью оценки угроз безопасности информации, будем считать, что функциональные компоненты данного (первого) уровня декомпозиции, рассматриваемой частной целевой функции, могут быть определены как тактики реализации доступа к отдельным СВТ:

– тактика внедрения ВПО (тактика $T_{1.1}^{(в)}$);

– тактика активации работы вредоносной программы (тактика $T_{1.2}^{(в)}$);

– тактика выявления вредоносной программой уязвимостей базовых компонент ПО, путем анализа их работы в операционной среде КС (тактика $T_{1.3}^{(в)}$);

– тактика получения высокого уровня доступа в операционной среде (тактика $T_{1.4}^{(в)}$);

– тактика обхода механизма резидентной антивирусной защиты путем скрытия активности вредоносных программ (тактика $T_{1.5}^{(в)}$);

– тактика обеспечения постоянного доступа ВПО к операционной среде КС путем ассоциирования с программами автозагрузки (тактика $T_{1.6}^{(в)}$);

– тактика обеспечения связи с контрольным сервером для управления процессами в операционной среде КС и сбора необходимых данных (тактика $T_{1.7}^{(в)}$).

В соответствии с терминологией ФСТЭК [8] будем считать, что функциональные компоненты данного (теперь уже второго) уровня декомпозиции, рассматриваемой частной целевой функции могут быть определены как техники, используемые в процессе реализации отдельных тактик доступа к СВТ.

Рассмотрим процедуру функциональной декомпозиции тактик на примере тактики выявления вредоносной программой уязвимостей базовых компонент ПО путем анализа их работы в операционной среде КС (тактики $Т_{1.3}^{(в)}$). Техниками, реализующими данную тактику, являются:

– техника сбора и анализа информации о пользователях, их привилегиях и параметрах учетных записей, а также членства в группах (техника $т_{1.3.1}^{(в)}$);

– техника сбора и анализа информации о правах доступа пользователей к ресурсам (техника $т_{1.3.2}^{(в)}$);

– техника выявления доступных опций и функций программного обеспечения (техника $т_{1.3.3}^{(в)}$);

– техника оценки функциональности компонент ПО (техника $т_{1.3.4}^{(в)}$);

– техника оценки возможностей взаимодействия ВПО с компонентами ПО (техника $т_{1.3.5}^{(в)}$);

– техника анализа активности процессов, выполняемых в операционной среде (техника $т_{1.3.6}^{(в)}$);

– техника оценки наличия и состояния антивирусного ПО и других средств защиты информации (техника $т_{1.3.7}^{(в)}$);

– техника выявления уязвимых приложений (техника $т_{1.3.8}^{(в)}$);

– техника получения списка файлов в файловой системе для выявления конфиденциальной информации (техника $т_{1.3.9}^{(в)}$);

– техника доступа к реестру ОС для извлечения конфигурационных данных и настроек СВТ (техника $т_{1.3.10}^{(в)}$);

– техника получения информации об аппаратных и программных характеристиках СВТ (техника $т_{1.3.11}^{(в)}$);

– техника сбора и анализа информации о сетевых параметрах СВТ (техника $т_{1.3.12}^{(в)}$);

– техника сбора и анализа информации о периферии (техника $т_{1.3.13}^{(в)}$).

Уровень техник является конечным уровнем декомпозиции как частной целевой функции «Доступ к отдельным СВТ – объектам вирусной атаки», так и общей целевой функции «Воздействие ВПО», который позволяет сформи-

ровать признаки воздействия ВПО на операционную среду КС, идентифицируемые соответствующими средствами диагностики ОС и антивирусными средствами. Данные признаки как признаки доступа к отдельным СВТ – объектам вирусной атаки, приводятся в табл. 1.

Таблица 1

Пространство признаков доступа к отдельным СВТ – объектам вирусной атаки

Наименование техники	Признак	Средство, идентифицирующее признак
1	2	3
1. Техника сбора и анализа информации о пользователях, их привилегиях и параметрах учетных записей, а также членства в группах	Сбор и анализ информации о пользователях, их привилегиях и параметрах учетных записей, а также членства в группах	PowerView для PowerShell
2. Техника сбора и анализа информации о правах доступа пользователей к ресурсам	Сбор и анализ информации о правах доступа пользователей к ресурсам	AccessEnum от Sysinternals
3. Техника выявления доступных опций и функций программного обеспечения	Выявление доступных опций и функций программного обеспечения	SonarQube; IDA Pro, Ghidra
4. Техника оценки функциональности компонент ПО	Оценка функциональности компонент ПО	Selenium: JUnit/TestNG; Postman; SonarQube: Checkstyle/PMD; Apache JMeter; LoadRunner:
5. Техника оценки возможностей взаимодействия ВПО с компонентами ПО	Оценка возможностей взаимодействия ВПО с компонентами ПО	Postman: SoapUI; Apache JMeter: Cypress: SonarQube; ESLint/TSLint: Elastic Stack (ELK); Prometheus и Grafana
6. Техника анализа активности процессов, выполняемых в операционной среде	Анализ активности процессов, выполняемых в операционной среде	Process Explorer или Sysinternals
7. Техника оценки наличия и состояния антивирусного ПО и других средств защиты информации	Оценка наличия и состояния антивирусного ПО и других средств защиты информации	AV-тест
8. Техника выявления уязвимых приложений	Выявление уязвимых приложений	Nessus; OpenVAS
9. Техника получения списка файлов в файловой системе для выявления конфиденциальной информации	Получение списка файлов в файловой системе для выявления конфиденциальной информации	Командная строка (cmd); PowerShel

Окончание табл. 1

1	2	3
10. Техника доступа к реестру ОС для извлечения конфигурационных данных и настроек СВТ	Доступ к реестру ОС для извлечения конфигурационных данных и настроек СВТ	Regedit или reg query
11. Техника получения информации об аппаратных и программных характеристиках СВТ	Получение информации об аппаратных и программных характеристиках СВТ	CPU-Z; Speccy
12. Техника сбора и анализа информации о сетевых параметрах СВТ	Сбор и анализ информации о сетевых параметрах СВТ	Wireshark
13. Техника сбора и анализа информации о периферии	Сбор и анализ информации о периферии	Диспетчер устройств; PowerShel

В соответствии со вторым этапом приведенной выше последовательности разработки математических моделей определим порядок реализации частной целевой функции «Доступ к отдельным СВТ – объектам вирусной атаки». Для этого воспользуемся методологией функционального моделирования IDEF0 [9], согласно которой рассматриваемые процессы представляются в виде функциональных диаграмм, на рис. 1 приводится порядок реализации, рассмотренной выше в качестве примера, тактики выявления вредоносной программой уязвимостей базовых компонент ПО, путем анализа их работы в операционной среде КС.

В соответствии с третьим этапом построения модели представим исследуемый процесс, описанный в терминах функциональных диаграмм как марковский. На рис. 2 приводится иллюстрация тактики выявления вредоносной программой уязвимостей базовых компонент ПО как марковского процесса.

В соответствии с четвертым этапом построения модели определяются временные характеристики отдельных функциональных компонент частной целевой функции «Доступ к отдельным СВТ – объектам вирусной атаки». Для этого воспользуемся соответствиями между временными характеристиками функциональных компонент данной целевой функции. Указанные соответствия, а следовательно, и вид аналитических моделей для временных характеристик функциональных компонент определяются содержанием межуровневых и внутриуровневых композиционных связей.

При построении аналитических моделей средних значений временных характеристик функциональных компонент целевой функции ВПО воспользуемся свойством аддитивности математического ожидания композиции случайных величин [10]. При этом для композиции случайных величин τ_1, τ_2, …, τ_N, характеризующих время реализации последовательности функциональных компонент 1, 2, …, N, воспользуемся выражением

$$\overline{\tau} = \sum_{n=1}^{N} \overline{\tau}_n , \qquad (2)$$

где $\overline{\tau}_n$ – среднее значение случайной величины τ_n.

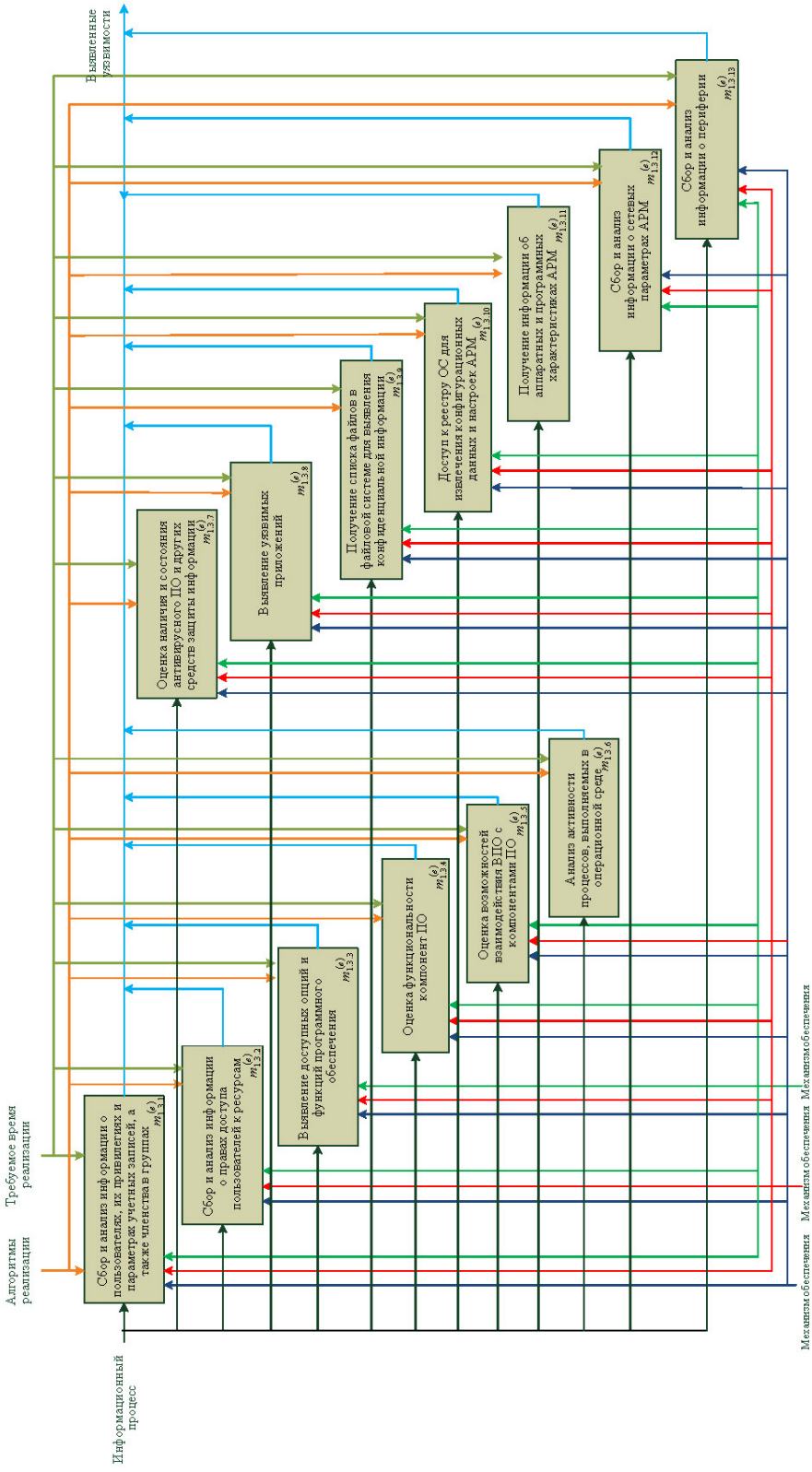

Рис. 1. Функциональная диаграмма тактики $T^{(в)}_{1.3}$ выявления вредоносных программных уязвимостей базовых компонент ПО

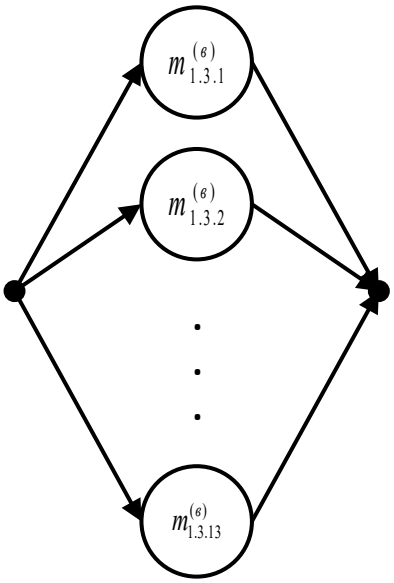

Рис. 2. Представление тактики $\mathrm{T}^{(\mathrm{в})}_{1.3}$ выявления вредоносной программой уязвимостей базовых компонент ПО в виде графа

В случае, когда функциональные компоненты 1, 2, …, *M*, связаны параллельно, для композиции случайных величин τ_1, τ_2, …, τ_M, характеризующих время их реализации, будем использовать выражение

$$\overline{\tau} = \sum_{m=1}^{M} p_{s,m} \cdot \overline{\tau}_m \,, \tag{3}$$

где $p_{s,m}$ и $\overline{\tau}_m$ – вероятность реализации *m*-й функциональной компоненты после *s*-й функциональной компоненты и среднее значение случайной величины τ_m времени ее реализации соответственно.

Из приведенного на рис. 2 формализованного представления тактики $\mathrm{T}^{(\mathrm{в})}_{1.3}$ выявления вредоносной программой уязвимостей базовых компонент ПО следует, что среднее значение случайной величины времени $\overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3}}$ ее выполнения определяется в соответствии с выражением

$$\begin{aligned}\overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3}} = {} & p_{1.1} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.1}} + p_{1.2} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.2}} + p_{1.3} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.3}} + p_{1.4} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.4}} + p_{1.5} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.5}} + \\ & + p_{1.6} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.6}} + p_{1.7} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.7}} + p_{1.8} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.8}} + p_{1.9} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.9}} + p_{1.10} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.10}} + \\ & + p_{1.11} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.11}} + p_{1.12} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.12}} + p_{1.13} \cdot \overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3.13}} \,; \end{aligned} \tag{1}$$

где $\overline{\tau}_{\mathrm{T}^{(\mathrm{в})}_{1.3}}$ – среднее значение времени реализации *m*-й, *m* = 1, 2, …, 13, техники тактики $\mathrm{T}^{(\mathrm{в})}_{1.3}$ выявления вредоносной программой уязвимостей базовых

компонент ПО; $p_{1.m}$ – вероятность того, что выполнение тактики $\mathrm{T}_{1.3}^{(\mathrm{в})}$ начнется с реализации $\mathrm{T}_{1.m}^{(\mathrm{в})}$ m-й, m = 1, 2, …, 13, техники.

Заключение

Очевидна универсальность четырехэтапной процедуры построения математических моделей для любого варианта функциональной декомпозиции процесса воздействия ВПО. Аналогичным образом могут быть описаны и остальные этапы декомпозиционной структуры целевой функции «Воздействие ВПО».

Принципиальная роль методического аппарата функционального моделирования состоит в том, что он обеспечивает существенное повышение адекватности этих моделей. Его применение позволяет избежать недостатков субъективного мнения экспертов при формировании формализованной картины угрозы воздействия ВПО, так как ориентирует на имеющиеся закономерности практики исследования такого рода угроз в виде последовательности действий нарушителя по реализации своей целевой функции.

Список источников

1. Мазин А. В., Гайфулин В. В. [и др.]. Теория информации как методологическая основа решения проблем адекватной оценки возможностей по обеспечению защиты информации // Известия Института инженерной физики. 2022. № 2 (64). С. 64–68.
2. Скрыль С. В., Хохлов Н. С. [и др.]. Информатика : учебник для высших учебных заведений МВД России. Информатика: Концептуальные основы. М. : Маросейка, 2008. Т. 1. 464 с.
3. Куприянов А. И., Коробец Б. Н., Бардаев Э. А., Королев И. Д. [и др.]. Теория информации: учебник / под. ред. С. В. Скрыля. М. : Изд. центр «Академия», 2020. 240 с.
4. Хартли Р. Передача информации // Теория информации и ее приложения : сб. переводов. М. : Гос. изд. физ.-мат. лит, 1959. С. 5–35.
5. Скрыль С. В., Стадник А. Н., Купин Д. С., Домрачев Д. В., Абачараева Э. Р. Функциональное моделирование как инструмент формализации угроз вирусных атак на информационные ресурсы компьютерных систем // Телекоммункации. 2021. № 4. С. 14–19.
6. Тихонов В. И., Миронов М. А. Марковские процессы. М. : Сов. радио, 1977. 488 с.
7. Калянов Г. Н. CASE: Структурный системный анализ (автоматизация и применение). М. : Лори, 1996. 242 с.
8. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации». Утверждена 5 февраля 2021 года. М. : ФСТЭК, 2021. 83 с.
9. Методология функционального моделирования IDEF0. Руководящий документ. М. : Изд-во стандартов, 2000. 75 с.
10. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). М. : Изд-во Наука, 1973. 832 с.

Reference

1. Mazin A.V., Gayfulin V.V. et al. Information theory as a methodological basis for solving problems of adequate assessment of capabilities to ensure information security. *Izvestiya Instituta inzhenernoy fiziki = Proceedings of Institute of Engineering Physics.* 2022;(2):64–68. (In Russ.)

2. Skryl' S.V., Khokhlov N.S. et al. *Informatika: uchebnik dlya vysshikh uchebnykh zavedeniy MVD Rossii. Informatika: Kontseptual'nye osnovy = Computer science: a textbook for Higher Education Institutions of the Ministry of Internal Affairs of Russia. Computer science: conceptual foundations*. Moscow: Maroseyka, 2008;1:464. (In Russ.)
3. Kupriyanov A.I., Korobets B.N., Bardaev E.A., Korolev I.D. et al. *Teoriya informatsii: uchebnik = Information theory: a textbook.* Moscow: Izd. tsentr «Akademiya», 2020:240. (In Russ.)
4. Khartli R. Transfer of information. *Teoriya informatsii i ee prilozheniya: sb. perevodov = Information theory and its applications: a collection of translations*. Moscow: Gos. izd. fiz.-mat. lit, 1959:5–35. (In Russ.)
5. Skryl' S.V., Stadnik A.N., Kupin D.S., Domrachev D.V., Abacharaeva E.R. Functional modeling as a tool for formalizing threats of virus attacks on information resources of computer systems. *Telekommunkatsii = Telecommunications*. 2021;(4):14–19. (In Russ.)
6. Tikhonov V.I., Mironov M.A. *Markovskie protsessy = Markov processes*. Moscow: Sov. radio, 1977:488. (In Russ.)
7. Kalyanov G.N. *CASE: Strukturnyy sistemnyy analiz (avtomatizatsiya i primenenie) = CASE: Structural Systems Analysis (Automation and Application).* Moscow: Lori, 1996:242. (In Russ.)
8. *Metodicheskiy dokument FSTEK Rossii «Metodika otsenki ugroz bezopasnosti informatsii». Utverzhdena 5 fevralya 2021 goda = FSTEC of Russia's Methodological Document "Methodology for Assessing Information Security Threats". Approved on February 5, 2021.* Moscow: FSTEK. 2021:83. (In Russ.)
9. *Metodologiya funktsional'nogo modelirovaniya IDEF0. Rukovodyashchiy document = IDEF0 Functional Modeling Methodology. Guidance Document*. Moscow: Izd-vo standartov, 2000:75. (In Russ.)
10. Korn G., Korn T. *Spravochnik po matematike (dlya nauchnykh rabotnikov i inzhenerov) = Handbook of mathematics (for scientists and engineers).* Moscow: Izd-vo Nauka, 1973:832. (In Russ.)

Информация об авторах / Information about the authors

Руслан Александрович Хворов
кандидат технических наук, старший преподаватель Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина» (Россия, Воронеж, ул. Ст. Большевиков, 54)

E-mail: khvoroff@rambler.ru

Ruslan A. Khvorov
Candidate of engineering sciences, senior lecturer of the Military Training and Scientific Center of the Air Force "Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin" (54 St. Bolshevikov street, Voronezh, Russia)

Кирилл Сергеевич Скрыль
кандидат юридических наук, доцент, доцент кафедры безопасности в цифровом мире, Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет) (Россия, г. Москва, ул. 2-я Бауманская, 5)

E-mail: kskryl@bmstu.ru

Kirill S. Skryl'
Candidate of juridical sciences, associate professor, associate professor of the sub-department of Security in the Digital World, Bauman Moscow State Technical University (National Research University) (5 Vtoraya Baumanskaya street, Moscow, Russia)

Игорь Игоревич Корчагин
руководитель группы обеспечения безопасности информации, АО «Информационная внедренческая компания» (Россия, г. Москва, ул. Бутырская, 75)

E-mail: korchagin@ivk.ru

Igor' I. Korchagin
Head of the Information Security Group, Information Implementation Company JSC (75 Butyrskaya street, Moscow, Russia)

Ксения Евгеньевна Амелина
кандидат юридических наук, доцент, доцент кафедры безопасности в цифровом мире, Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет) (Россия, г. Москва, ул. 2-я Бауманская, 5)

E-mail: amelina@bmstu.ru

Kseniya E. Amelina
Candidate of juridical sciences, associate professor, associate professor of the sub-department of Security in the Digital World, Bauman Moscow State Technical University (National Research University) (5 Vtoraya Baumanskaya street, Moscow, Russia)

Виктор Валерьевич Гайфулин
кандидат технических наук, доцент кафедры № 34, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко (Россия, г. Краснодар, ул. Красина, 4)

E-mail: gayfulin2007@yandex.ru

Viktor V. Gayfulin
Candidate of engineering sciences, associate professor of the sub-department No. 34, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko (4 Krasina street, Krasnodar, Russia)

Игорь Васильевич Савельев
кандидат технических наук, доцент кафедры № 34, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко (Россия, г. Краснодар, ул. Красина, 4)

E-mail: kvvu@mil.ru

Igor' V. Savel'ev
Candidate of engineering sciences, associate professor of the sub-department No. 34, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko (4 Krasina street, Krasnodar, Russia)

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflicts of interests.

Поступила в редакцию / Received 11.06.2025

Поступила после рецензирования и доработки / Revised 29.08.2025

Принята к публикации / Accepted 12.09.2025