УДК 004.942
doi: 10.21685/2072-3059-2025-3-4

Методология функционального моделирования как инструмент разработки адекватных математических моделей процессов обеспечения антивирусной защиты в компьютерных системах

Р. А. Хворов[1], К. С. Скрыль[2], И. И. Корчагин[3], К. Е. Амелина[4]

[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

[1]khvoroff@rambler.ru, [2]kskryl@bmstu.ru, [3]korchagin@ivk.ru, [4]amelina@bmstu.ru

Аннотация. *Актуальность и цели.* Одним из направлений решения проблемы повышения адекватности математических моделей процессов обеспечения антивирусной защиты в компьютерных системах (КС) является формализация этих процессов с использованием методического аппарата функционального моделирования. Цель – разработка процедуры построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в компьютерных системах с использованием методического аппарата функционального моделирования. *Результаты.* Обоснована и реализована процедура построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС, включающая: этап детализации целевой функции «Антивирусная защита», этап установления порядка выполнения ее функциональных компонент на каждом из уровней декомпозиции, этап представления модели в виде графов и этап формирования аналитических выражений для оценки временных характеристик процессов обеспечения антивирусной защиты в КС. *Выводы*. Достигаемая за счет функциональной декомпозиции целевой функции «Антивирусная защита» адекватность математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС дает возможность научного обоснования требований к направлениям совершенствования соответствующих механизмов защиты.

Ключевые слова: функциональное моделирование, марковский процесс, антивирусная защита, математические модели процессов обеспечения антивирусной защиты в компьютерных системах

Для цитирования: Хворов Р. А., Скрыль К. С., Корчагин И. И., Амелина К. Е. Методология функционального моделирования как инструмент разработки адекватных математических моделей процессов обеспечения антивирусной защиты в компьютерных системах // Известия высших учебных заведений. Поволжский регион. Технические науки. 2025. № 3. С. 63–73. doi: 10.21685/2072-3059-2025-3-4

Functional modeling methodology as a tool for developing adequate mathematical models of antivirus protection processes in computer systems

R.A. Khvorov[1], K.S. Skryl'[2], I.I. Korchagin[3], K.E. Amelina[4]

[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
[1]khvoroff@rambler.ru, [2]kskryl@bmstu.ru, [3]korchagin@ivk.ru, [4]amelina@bmstu.ru

Abstract. *Background.* One of the directions for solving the problem of increasing the adequacy of mathematical models of processes for ensuring anti-virus protection in computer systems (CS) is the formalization of these processes using the methodological apparatus of functional modeling. The purpose of the study is to develop a procedure for constructing mathematical models of the temporal characteristics of processes providing anti-virus protection in computer systems using the methodological apparatus of functional modeling. *Results.* The procedure for constructing mathematical models of the temporal characteristics of the processes of providing anti-virus protection in the CS is substantiated and implemented, including: the stage of detailing the objective function "Anti-virus protection", the stage of establishing the order of execution of its functional components at each of the decomposition levels, the stage of presenting the model in the form of graphs and the stage of forming analytical expressions for assessing the temporal characteristics of the processes of providing antivirus protection in the CS. *Conclusions*. The adequacy of mathematical models of the time characteristics of the processes of providing anti-virus protection in the CS, achieved through the functional decomposition of the objective function "Anti-virus protection", makes it possible to scientifically substantiate the requirements for the directions of improvement of the corresponding protection mechanisms.

Keywords: functional modeling, Markov process, antivirus protection, mathematical models of antivirus protection processes in computer systems

For citation: Khvorov R.A., Skryl' K.S., Korchagin I.I., Amelina K.E. Functional modeling methodology as a tool for developing adequate mathematical models of antivirus protection processes in computer systems. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki = University proceedings. Volga region. Engineering sciences.* 2025;(3):63–73. (In Russ.). doi: 10.21685/2072-3059-2025-3-4

Введение

Важнейшим фактором достижения корректности решения научных задач в сфере предотвращения угроз воздействия вредоносного программного обеспечения (ВПО) на информацию в компьютерных системах (КС) является высокая адекватность математических моделей, используемых для оценки временных характеристик как самих угроз, так и механизмов антивирусной защиты в этих системах [1]. Именно временные характеристики этих механизмов являются значимым фактором как эффективного обеспечения защиты информации в КС, так и эффективного функционирования КС в целом.

Среди множества существующих подходов к оценке адекватности математических моделей выделяется подход [2, 3], в основу которого положена концепция измерения количества информации, на которой базируется современная теория информации [4]. В основе такого подхода лежит восприятие модели объекта как источника знаний о нем. Естественно полагать, что чем больше информации об объекте генерирует модель, тем она более адекватна. Одним из вариантов реализации этой идеи может служить метрика Хартли [5], дающая возможность определить количество информации об объекте путем оценки числа идентифицируемых состояний, которые принимает данный объект. Соответствующее выражение имеет вид

$$K = \log_2(C), \quad (1)$$

где K – количество информации об объекте, C – число идентифицируемых состояний объекта.

Если предположить в качестве инструмента идентификации состояния объекта его модель, то выражение (1) можно рассматривать как выражение для оценки адекватности такой модели. Из чего следует, что чем большее число состояний исследуемого объекта описывает модель, тем выше ее адекватность.

Отсюда очевидным становится требование обеспечения на этапе формализации исследуемых процессов идентификации как можно большего числа их состояний.

Построение математических моделей временных характеристик процессов обеспечения антивирусной защиты в компьютерных системах

Существующая практика исследований в области моделирования, включая моделирование в приложениях теории информационной безопасности [6], дает основание полагать, что в качестве методологического аппарата для реализации данного требования может быть применен аппарат функционального моделирования. С этой целью рассмотрим процесс построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС, базовыми этапами которого являются этапы формализации этих процессов методами функционального моделирования.

На первом этапе процедуры построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС путем детализации целевой функции «Антивирусная защита» образуются уровни ее функциональной декомпозиции. При этом исходя из причинно-следственных отношений предполагается, что детализация данной целевой функции будет соответствовать детализации целевой функции «Воздействие ВПО».

На втором этапе устанавливается порядок реализации (выполнения) функциональных компонент на каждом из уровней декомпозиции рассматриваемой целевой функции. При этом характер взаимосвязей между компонентами определяется эмпирически. Формируемые таким образом функциональные модели процесса антивирусной защиты в операционной среде компьютерной сети описываются терминами функциональных диаграмм [7].

На третьем этапе модели описание механизмов антивирусной защиты, иллюстрируемое функциональными диаграммами, представляется в виде графов, отражающих процесс антивирусной защиты в операционной среде КС как марковский [8].

На четвертом этапе формируются аналитические выражения для оценки временных характеристик отдельных функциональных компонент механизма антивирусной защиты.

В соответствии с первым этапом приведенной выше последовательности разработки адекватных математических моделей процессов обеспечения антивирусной защиты путем детализации соответствующей целевой функции «Антивирусная защита» дадим ее структурное представление. Такое представление является способом отражения специалистами в области компьютерной вирусологии их эмпирических знаний о порядке реализации механизмов антивирусной защиты.

Исходя из динамики достижения целей реализации этих механизмов должностными лицами, ответственными за обеспечение безопасности ин-

формации в КС, необходимо проанализировать источники потенциальной угрозы воздействия ВПО, состояние и поведение операционной среды КС, а также отреагировать на вредоносную активность ВПО [9].

Определим эти действия как функциональные компоненты первого уровня декомпозиции целевой функции «Антивирусная защита» или этапы ее реализации:

– этап анализа источников потенциальной угрозы воздействия ВПО (этап $Э_1^{(з)}$);

– этап анализа состояния операционной среды и ее поведения (этап $Э_2^{(з)}$);

– этап реагирования на вредоносную активность (этап $Э_3^{(з)}$).

Этап $Э_1^{(з)}$ составляют следующие функциональные компоненты процесса анализа источников потенциальной угрозы воздействия ВПО:

– тактика анализа входящих и исходящих сообщений на наличие вредоносных вложений, ссылок, признаков фишинга (тактика $Т_{1.1}^{(з)}$);

– тактика анализа доменных имен, IP- и URL-адресов для обнаружения вредоносной активности (тактика $Т_{1.2}^{(з)}$);

– тактика анализа сетевого трафика с целью обнаружения признаков вредоносной активности (тактика $Т_{1.3}^{(з)}$);

– тактика анализа файлов на наличие вредоносного кода, аномалий и других признаков компрометации (тактика $Т_{1.4}^{(з)}$).

Второй этап – этап $Э_2^{(з)}$ – составляют следующие функциональные компоненты процесса анализа состояния операционной среды и ее поведения:

– тактика анализа активных процессов на наличие аномалий, подозрительного поведения и несанкционированной активности (тактика $Т_{2.1}^{(з)}$);

– тактика анализа системных компонент (драйверов, библиотек, реестров) на наличие признаков компрометации и вредоносной активности (тактика $Т_{2.2}^{(з)}$);

– тактика анализа поведения пользователей в операционной среде КС с целью выявления вредоносной активности (тактика $Т_{2.3}^{(з)}$).

Завершающий реализацию целевой функции этап – этап $Э_3^{(з)}$ – составляют следующие функциональные компоненты процесса реагирования на вредоносную активность: тактика реагирования на уровне процесса (тактика $Т_{3.1}^{(з)}$) и на уровне данных (тактика $Т_{3.2}^{(з)}$).

В отличие от декомпозиции целевой функции «Воздействие ВПО», где уровень тактик, являясь источником признаков реализации вредоносного воздействия, определяет данный уровень как конечный уровень декомпозиции, для механизмов антивирусной защиты наличие или отсутствие признаков реализации этих механизмов не влияет на процесс защиты. Воспользо-

вавшись принципом структурной идентичности и функциональной противоположности целевых функций «Воздействие ВПО» и «Антивирусная защита», уровень тактик определим как конечный уровень декомпозиции для обеих целевых функций.

В соответствии со вторым этапом приведенной выше последовательности построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС путем детализации целевой функции «Антивирусная защита» определим порядок реализации ее функциональных компонент. Для этого воспользуемся методологией функционального моделирования IDEF0 [10], согласно которой рассматриваемые процессы представляются в виде функциональных диаграмм (рис. 1–4).

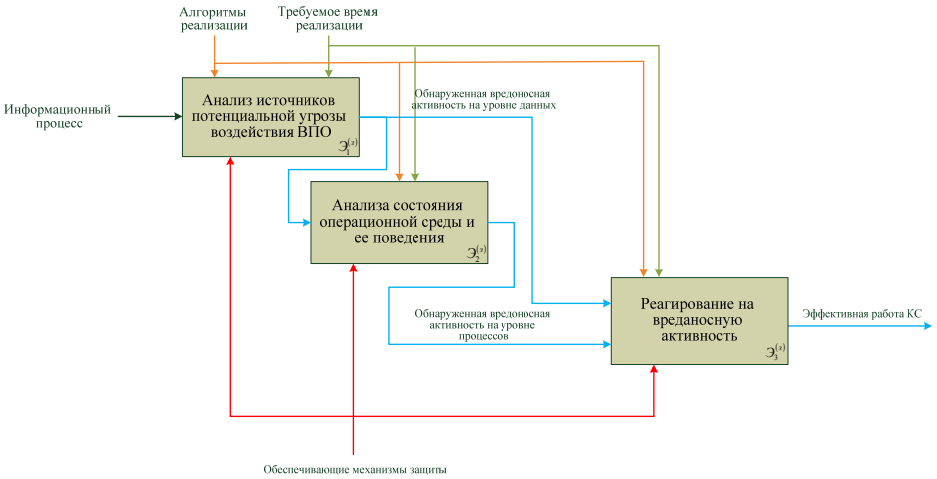

Рис. 1. Функциональная диаграмма целевой функции «Антивирусная защита»

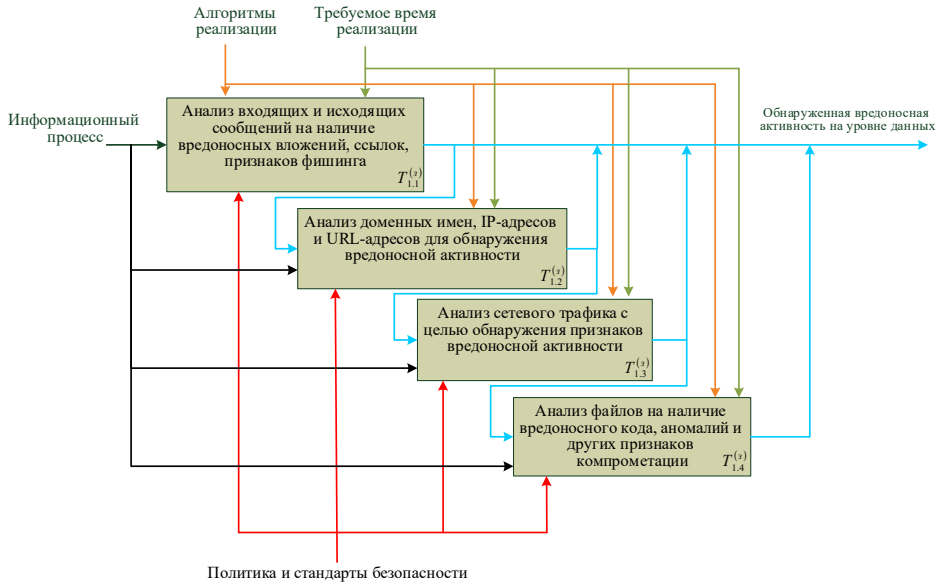

Рис. 2. Функциональная диаграмма этапа $Э_1^{(з)}$
анализа источников потенциальной угрозы воздействия ВПО

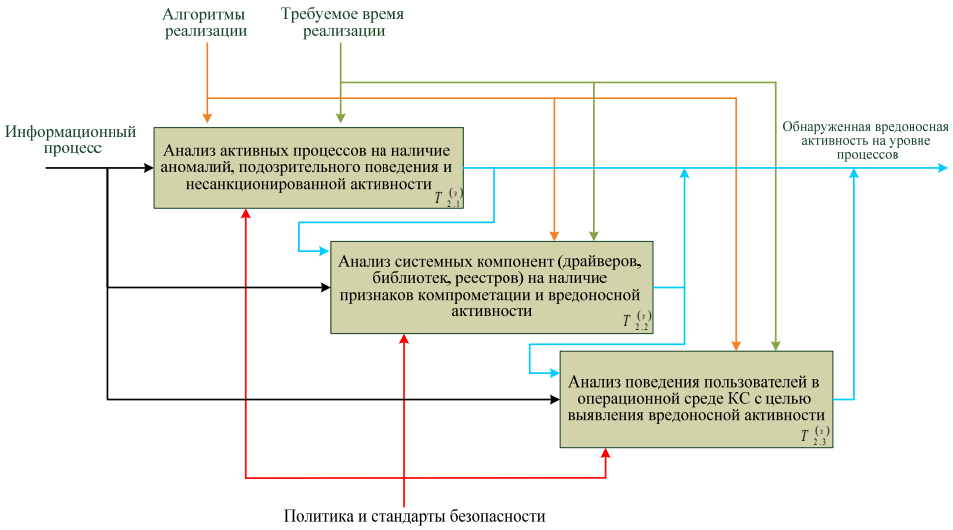

Рис. 3. Функциональная диаграмма этапа $Э_2^{(з)}$
анализа состояния операционной среды и ее поведения

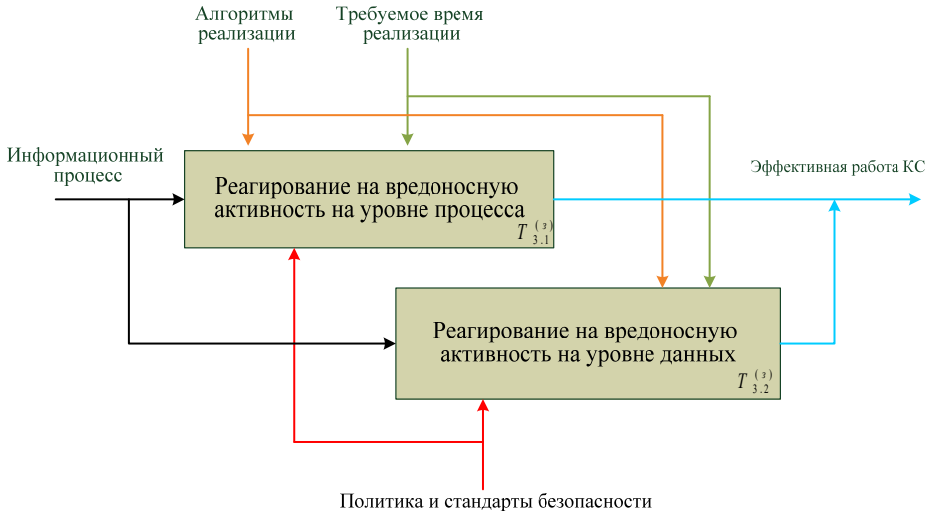

Рис. 4. Функциональная диаграмма этапа $Э_3^{(з)}$
реагирования на вредоносную активность

В соответствии с третьим этапом построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС описание механизмов антивирусной защиты, иллюстрируемое функциональными диаграммами (рис. 1–4), представляется в виде графов, отражающих процесс антивирусной защиты в операционной среде КС как марковский (рис. 5–8).

В соответствии с четвертым этапом построения математических моделей временных характеристик процессов обеспечения антивирусной защиты в КС при их определении воспользуемся функциональными соответствиями между тактиками, применяемыми в рамках отдельных этапов защиты, и меж-

ду этими этапами в процессе реализации целевой функции «Антивирусная защита». Указанные соответствия, а следовательно, и вид аналитической модели для этих характеристик определяются содержанием их композиционных связей.

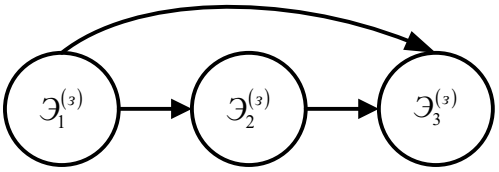

Рис. 5. Представление целевой функции «Антивирусная защита» в виде марковского процесса

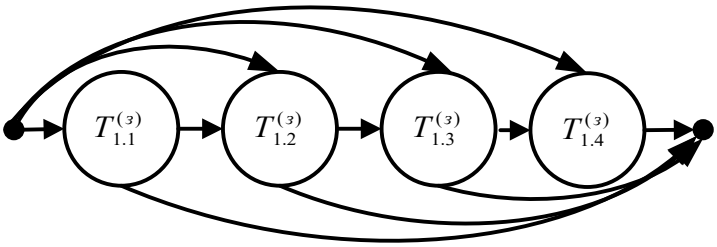

Рис. 6. Представление этапа анализа источников потенциальной угрозы воздействия ВПО в виде марковского процесса

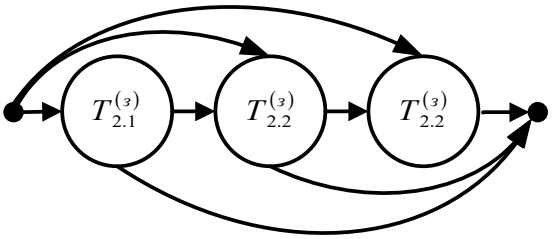

Рис. 7. Представление этапа анализа состояния операционной среды и ее поведения в виде марковского процесса

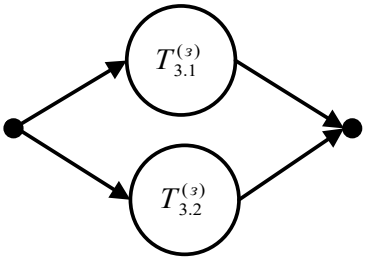

Рис. 8. Представление этапа реагирования на вредоносную активность в виде марковского процесса

При построении аналитических моделей средних значений временных характеристик этапов и самой целевой функции «Антивирусная защита» воспользуемся свойством линейности и аддитивности, математического ожида-

ния композиции случайных величин [11]. При этом для композиции случайных величин τ_1, τ_2, …, τ_N, характеризующих время реализации последовательности функциональных компонент 1, 2, …, N, воспользуемся выражением

$$\overline{\tau} = \sum_{n=1}^{N} \overline{\tau}_n \,, \tag{2}$$

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

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.

Исходя из приведенного на рис. 6 формализованного представления этапа анализа источников потенциальной угрозы воздействия ВПО среднее значение случайной величины времени $\overline{\tau}_{Э_1^{(з)}}$ его выполнения определяется в соответствии с выражением

$$\begin{aligned}\overline{\tau}_{Э_1^{(з)}} = p_{1.1} \cdot \left(\overline{\tau}_{T_{1.1}^{(з)}} + p_{1.1,1.2} \cdot \left(\overline{\tau}_{T_{1.2}^{(з)}} + p_{1.2,1.3} \cdot \left(\overline{\tau}_{T_{1.3}^{(з)}} + p_{1.4} \cdot \overline{\tau}_{T_{1.4}^{(з)}} \right) \right) \right) + \\ + p_{1.2} \cdot \left(\overline{\tau}_{T_{1.2}^{(з)}} + p_{1.2,1.3} \cdot \left(\overline{\tau}_{T_{1.3}^{(з)}} + p_{1.4} \cdot \overline{\tau}_{T_{1.4}^{(з)}} \right) \right) + \\ + p_{1.3} \cdot \left(\overline{\tau}_{T_{1.3}^{(з)}} + p_{1.4} \cdot \overline{\tau}_{T_{1.4}^{(з)}} \right) + p_{1.4} \cdot \overline{\tau}_{T_{1.4}^{(з)}} ;\end{aligned} \tag{4}$$

где $\overline{\tau}_{T_{1.m}^{(з)}}$ – среднее значение времени реализации m, m = 1, 2, …4, тактики этапа $Э_1^{(з)}$ анализа источников потенциальной угрозы; $p_{1.i}$ – вероятность выполнения i-й тактики этапа $Э_1^{(з)}$; $p_{1.i,1.j}$ – вероятность выполнения j-й тактики после завершения i-й тактики этапа $Э_1^{(з)}$.

Исходя из приведенного на рис. 7 формализованного представления этапа анализа состояния операционной среды и ее поведения среднее значение случайной величины времени $\overline{\tau}_{Э_2^{(з)}}$ его выполнения определяется в соответствии с выражением

$$\overline{\tau}_{Э_2^{(з)}} = p_{2.1} \cdot \left(\overline{\tau}_{T_{2.1}^{(з)}} + p_{2.1,2.2} \cdot \left(\overline{\tau}_{T_{2.2}^{(з)}} + p_{2.3} \cdot \overline{\tau}_{T_{2.3}^{(з)}} \right) \right) +$$

$$+p_{2.2}\cdot\left(\overline{\tau}_{\mathrm{T}_{2.2}^{(з)}}+p_{2.3}\cdot\overline{\tau}_{\mathrm{T}_{2.3}^{(з)}}\right)+p_{2.3}\cdot\overline{\tau}_{\mathrm{T}_{2.3}^{(з)}}, \quad (5)$$

где $\overline{\tau}_{\mathrm{T}_{2.m}^{(з)}}$ – среднее значение времени реализации m, m = 1, 2, 3, тактик этапа $\mathrm{Э}_2^{(з)}$ анализа состояния операционной среды и ее поведения; $p_{2.i}$ – вероятность выполнения i-й тактики этапа $\mathrm{Э}_2^{(з)}$; $p_{2.i,2.j}$ – вероятность выполнения j-й тактики после завершения i-й тактики этапа $\mathrm{Э}_2^{(з)}$.

Исходя из приведенного на рис. 8 формализованного представления этапа реагирования на вредоносную активность среднее значение случайной величины времени $\overline{\tau}_{\mathrm{Э}_3^{(з)}}$ его выполнения определяется в соответствии с выражением

$$\overline{\tau}_{\mathrm{Э}_3^{(з)}}=p_{3.1}\cdot\overline{\tau}_{\mathrm{T}_{3.1}^{(з)}}+p_{3.2}\cdot\overline{\tau}_{\mathrm{T}_{3.2}^{(з)}}, \quad (6)$$

где $\overline{\tau}_{\mathrm{T}_{3.m}^{(в)}}$ – среднее значение времени реализации m, m = 1, 2, тактик этапа $\mathrm{Э}_3^{(в)}$ нарушения состояния защищенности информации; $p_{3.1}$ и $p_{3.2}$ – вероятность выполнения тактик $\mathrm{T}_{3.1}^{(з)}$ и $\mathrm{T}_{3.2}^{(з)}$ этапа $\mathrm{Э}_3^{(з)}$ соответственно.

Исходя из приведенного на рис. 5 формализованного представления целевой функции «Антивирусная защита» среднее значение случайной величины времени $\overline{\tau}_{(АВЗ)}$ ее выполнения определяется в соответствии с выражением

$$\overline{\tau}_{(\mathrm{АВЗ})}=\overline{\tau}_{\mathrm{Э}_1^{(з)}}+p_{1,2}\cdot\left(\overline{\tau}_{\mathrm{Э}_2^{(з)}}+\overline{\tau}_{\mathrm{Э}_3^{(з)}}\right)+p_{1,3}\cdot\overline{\tau}_{\mathrm{Э}_3^{(з)}}, \quad (7)$$

где $\overline{\tau}_{\mathrm{Э}_1^{(з)}}$, $\overline{\tau}_{\mathrm{Э}_2^{(з)}}$ и $\overline{\tau}_{\mathrm{Э}_3^{(з)}}$ соответствует выражениям (4), (5) и (6); $p_{1,2}$ и $p_{1,3}$ – вероятность выполнения этапа $\mathrm{Э}_2^{(з)}$ после $\mathrm{Э}_1^{(з)}$ и этапа $\mathrm{Э}_3^{(з)}$ после $\mathrm{Э}_1^{(з)}$.

Заключение

Таким образом, очевидно, что обеспечение выполнения высоких требований к адекватности математических моделей антивирусной защиты возможно путем использования методического аппарата функционального моделирования как средства первичной формализации исследуемых процессов. Его применение позволяет формализовать эмпирику исследователя, проявляющуюся вследствие субъективного понимания процесса антивирусной защиты.

Список литературы

1. Касперский Е. В. Компьютерное zловредство. СПб. : Питер, 2007. 208 с.
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. Сычев А. М., Скрыль С. В., Никулин С. С., Пономарёв М. В. [и др.]. Показатели адекватности структурированных систем оценки характеристик информационных процессов // Промышленные АСУ и контроллеры. 2017. № 2. С. 50–53.
4. 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.
5. Хартли Р. Передача информации // Теория информации и ее приложения : сб. переводов. М. : Гос. изд. физ.-мат. лит, 1959. С. 5–35
6. 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 // Телекоммуникации. 2021. № 4. С. 14–19.
7. Калянов Г. Н. CASE: Структурный системный анализ (автоматизация и применение). М. : Лори, 1996. 242 с.
8. Тихонов В. И., Миронов М. А. Марковские процессы. М. : Сов. радио, 1977. 488 с.
9. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации». Утверждена 5 февраля 2021 года. М. : ФСТЭК, 2021. 83 с.
10. Методология функционального моделирования IDEF0. Руководящий документ. М. : Изд-во стандартов, 2000. 75 с.
11. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). М. : Наука, 1973. 832 с.

Reference

1. Kasperskiy E.V. *Komp'yuternoe zlovredstvo = Computer malware*. Saint Petersburg: Piter, 2007:208. (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. Sychev A.M., Skryl' S.V., Nikulin S.S., Ponomarev M.V. et al. Indicators of the adequacy of structured systems for assessing the characteristics of information processes. *Promyshlennye ASU i kontrollery = Industrial control systems and controllers.* 2017;(2):50–53. (In Russ.)
4. 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.)
5. 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.)
6. 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.)
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. Tikhonov V.I., Mironov M.A. *Markovskie protsessy = Markov processes*. Moscow: Sov. radio, 1977:488. (In Russ.)
9. *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.)

10. *Metodologiya funktsional'nogo modelirovaniya IDEF0. Rukovodyashchiy document = IDEF0 Functional Modeling Methodology. Guidance Document*. Moscow: Izd-vo standartov, 2000:75. (In Russ.)
11. Korn G., Korn T. *Spravochnik po matematike (dlya nauchnykh rabotnikov i inzhenerov) = Handbook of Mathematics (for scientists and engineers)*. Moscow: 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)

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

Поступила в редакцию / Received 07.05.2025

Поступила после рецензирования и доработки / Revised 16.06.2025

Принята к публикации / Accepted 23.08.2025