Алексей В. Астрахов[1], Александр Н. Стадник[2], Кирилл С. Скрыль[3],
Иван И. Коровин[4], Эльвира Р. Башаева[5]
[1,3,4,5]Московский государственный технический университет им. Н.Э. Баумана,
2-я Бауманская ул., 5, стр. 4, Москва, 105005, Россия
[2]Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,
ул. Красина, 4, Краснодар, 350063, Россия
[1]e-mail: astrahov@bmstu.ru, https://orcid.org/0000-0003-0807-8884
[2]e-mail: alstaff@yandex.ru, https://orcid.org/0000-0003-0870-8057
[3]e-mail: Vorkir@mail.ru, https://orcid.org/0000-0001-6076-6970
[4]e-mail: korovin@ivk.ru, https://orcid.org/0000-0003-3233-7778
[5]e-mail: elvira.abacharaeva@yandex.ru, https://orcid.org/0000-0002-8885-1779

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ АНТИВИРУСНЫМИ СРЕДСТВАМИ ВРЕМЕННЫХ РЕСУРСОВ КОМПЬЮТЕРНОЙ СИСТЕМЫ

DOI: http://dx.doi.org/10.26583/bit.2023.1.05

Аннотация. Данная статья посвящена исследованию факторов, влияющих на своевременность реагирования на воздействия вредоносного программного обеспечения (ВПО). Проведен анализ средств антивирусной защиты в компьютерных системах (КС), основанный на экспертных оценках мер защиты от воздействия ВПО и экспертной оценки временных параметров антивирусных средств. Определены и обоснованы требования к временным характеристикам антивирусных средств в КС. В статье приводятся варианты формального представления характеристик для оценки реализации информационных процессов в КС и своевременности реагирования на воздействия ВПО. Анализируются характеристики, уточняющие модель угрозы безопасности информации в КС за счет учета специфики применения ВПО. Дается обоснование математической абстракции для формального представления последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, получены аналитические выражения для оценки мер антивирусной защиты и действий нарушителя по реализации несанкционированного доступа. Формулируются и доказываются гипотезы относительно адекватности использования антивирусными средствами временного ресурса КС.

Ключевые слова: вредоносное программное обеспечение, компьютерная система, антивирусные средства, защита информации, несанкционированный доступ.

Для цитирования: АСТРАХОВ Алексей В. и др. ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ АНТИВИРУСНЫМИ СРЕДСТВАМИ ВРЕМЕННЫХ РЕСУРСОВ КОМПЬЮТЕРНОЙ СИСТЕМЫ. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 70–80, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1475. DOI: http://dx.doi.org/10.26583/bit.2023.1.05.

Alexey V. Astrakhov[1], Alexander N. Stadnik[2], Kirill S. Skryl[3],
Ivan I. Korovin[4], Elvira R. Bashaeva[5]
[1,3,4,5]Moscow State Technical University,
2nd Baumanskaya Str., 5, p. 4, Moscow, 105005, Russia
[2]Krasnodar Higher Military School named after Army General S.M. Shtemenko,
Krasin Str., 4, Krasnodar, 350063, Russia
[1]e-mail: astrahov@bmstu.ru, https://orcid.org/0000-0003-0807-8884
[2]e-mail: alstaff@yandex.ru, https://orcid.org/0000-0003-0870-8057
[3]e-mail: Vorkir@mail.ru, https://orcid.org/0000-0001-6076-6970
[4]e-mail: korovin@ivk.ru, https://orcid.org/0000-0003-3233-7778
[5]e-mail: elvira.abacharaeva@yandex.ru, https://orcid.org/0000-0002-8885-1779

Exploration of the use of temporary computer system resources by anti-virus tools

DOI: http://dx.doi.org/10.26583/bit.2023.1.05

Abstract. The paper is devoted to the study of factors affecting the timeliness of response to the effects of malicious software. The analysis of anti-virus protection tools in computer systems is carried out. The analysis is based on expert assessments of protection measures against the effects of malicious software and expert assessment of the time parameters of anti-virus tools. The requirements for the time characteristics of anti-virus tools in the computer systems are defined and justified. The paper provides options for the formal presentation of characteristics for assessing the implementation of information processes in the computer systems and the timeliness of responding to the effects of the malicious software. The characteristics that clarify the model of information security threat in the computer systems are analyzed by taking into account the specifics of the use of the malicious software. The substantiation of mathematical abstraction for the formal representation of a sequence of random events associated with the implementation of the threat of the impact of the malicious software on the computer systems is given, analytical expressions are obtained to evaluate anti-virus protection measures and the actions of the violator to implement unauthorized access. Hypotheses are formulated and proved regarding the adequacy of the use of a temporary computer systems resource by antivirus tools.

Keywords: malicious software, computer system, antivirus tools, information protection, unauthorized access.

For citation: ASTRAKHOV Alexey V. et al. Exploration of the use of temporary computer system resources by antivirus tools. IT Security (Russia), [S.l.], v. 30, no. 1, p. 70–80, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1475. DOI: http://dx.doi.org/10.26583/bit.2023.1.05.

Введение

Характерная современному обществу устойчивая тенденция внедрения инфокоммуникационных технологий является фактором существенного повышения эффективности информационной и, как следствие, предметной деятельности. Вместе с тем эта тенденция явилась и источником целого ряда проблем, связанных с объективно существующими уязвимостями информации в компьютерных системах (КС) [1]. Подобного рода уязвимости обусловлены как большими объемами накапливаемых и обрабатываемых данных, так и сетевой технологией сбора и обработки информации в КС.

Уязвимости информации в КС обусловливают те или иные возможности для нарушителей ее безопасности по реализации соответствующих угроз. При этом одним из наиболее широко используемых нарушителями и серьезных, по своей сути, инструментов реализации угроз безопасности информации в КС является вредоносное программное обеспечение (ВПО) [2–4].

Возникновение ВПО связано с появлением и развитием в теории и практике программирования направления известного как «компьютерная вирусология». Термин «вирус», присутствующий в названии соответствующих программных продуктов, такие программы приобрели благодаря проявлению свойств ассоциативности, репликативности и полиморфизма, т.е. тех свойств, которые характерны вирусам в живой природе [3, 5].

Выработка мер обеспечения защиты от ВПО, адекватных требованиям своевременного реагирования на угрозы нарушения конфиденциальности, целостности и доступности информации и особенностям функционирования КС, привела к разработке соответствующих средств. Несмотря на то, что ВПО, на современном уровне его развития, включает и программные продукты, построенные на технологиях, не относящихся к вирусным [4, 6], существующая терминология в сфере информационной безопасности традиционно определяет средства защиты от воздействия ВПО как антивирусные средства. Особенностью этих средств является выполнение функций защиты от воздействия ВПО в процессе обработки информации в КС. Это приводит к необходимости совместного использования операционной среды [7] этих систем, их программным обеспечением (ПО) и антивирусными средствами. Подобная ситуация, естественным

образом, приводит к отвлечению определенной части временного ресурса КС на выполнение функций защиты от воздействия ВПО.

Поэтому весьма остро ставится проблема адекватного использования антивирусными средствами временного ресурса КС с целью обеспечения требуемого уровня безопасности обрабатываемой информации [8].

1. Существующее состояние вопросов исследования процессов обеспечения антивирусной защиты

Анализ существующей теоретической базы по вопросам исследования средств антивирусной защиты в КС дает основание утверждать, что сформировавшийся к настоящему времени методический аппарат не позволяет с должной степенью обеспечить адекватность обоснования технологий использования антивирусных средств. Главной причиной этого является эвристическое представление об адекватности существующих моделей исследуемым процессам, основанное на экспертных оценках выявленных закономерностей практики обеспечения безопасности информации.

На практике это приводит к тому, что нормативно определенные параметры применения антивирусных средств – периодичность и время выполнения процедур защиты от воздействия ВПО, вследствие экспертного характера оценки необходимости реализации мер защиты и экспертной оценки этих параметров, не обеспечивают требуемую адекватность реагирования на воздействия ВПО. Следствием этого является ситуация, когда требуемый уровень защищенности информации от ВПО в КС, не обеспечивается [9].

Субъективный характер выдвигаемых оценочных гипотез относительно аналогий эмпирического представления технологий использования антивирусных средств их реальным возможностям, не позволяет устанавливать объективное соответствие собственных временных параметров этих средств временным параметрам информационных процессов в КС в рассматриваемых условиях [10, 11].

Альтернативой субъективизму экспертного подхода к оценке временных параметров мер антивирусной защиты служит формализм методов математического моделирования [12], что, в свою очередь, приводит к необходимости формулировки соответствующих гипотез об аналогиях реальных процессов определенным математическим абстракциям [13].

С целью построения моделей временных характеристик применяемых мер антивирусной защиты, учитывающих указанный недостаток существующего методического аппарата обоснования временных параметров применения антивирусных средств, сформулируем гипотезы, которые могут быть использованы в качестве теоретических положений для совершенствования данного методического аппарата.

2. Гипотеза об адекватности характеристик мер антивирусной защиты характеристикам процессов накопления, обработки и обмена данными в КС

Формулировка гипотезы: существует соответствие между значением характеристики своевременности реализации информационных процессов в КС и значением характеристики своевременности реагирования на воздействия ВПО средствами антивирусной защиты.

С целью доказательства гипотезы дадим формальную интерпретацию упомянутых характеристик.

Исходя из того, что характеристика своевременности реализации информационных процессов в КС отражает возможности данной системы по реализации своей целевой

функции [14], определим ее как нормированную характеристику времени τ реализации информационных процессов в КС в условиях воздействия ВПО и мер антивирусной защиты. При этом, нормирование проводится относительно максимально допустимой величины $\tau_{\max}$ времени τ. Формально это можно представить условиями:

$$\tau \le \tau_{\max} \tag{1}$$

и

$$\tau > \tau_{\max}, \tag{2}$$

где τ и $\tau_{\max}$ – время реализации информационных процессов в КС и их максимально допустимыми значениями.

Величина $\tau_{\max}$ определяется нормативными требованиями к продолжительности обработки информации в КС.

Будем полагать, что условие (1) является обязательным требованием к реализации процедур накопления, обработки и обмена данными в КС. В противном случае (условие (2)) целевая функция КС не достигается.

В общем случае обе входящие в неравенства (1) и (2) величины являются случайными, поэтому их выполнение являются случайными событиями. Вероятность события $P(\tau \le \tau_{\max})$ представляет собой среднее количество циклов обработки информации в КС, своевременно реализованных данной системой на временном отрезке $[t_1, t_2]$ относительно их общего числа:

$$P(\tau \le \tau_{\max}) = \frac{1}{N} \cdot \sum_{n=1}^{N} \alpha_n , \tag{3}$$

где $$\alpha_m = \begin{cases} 1, \textit{ при } \tau_{(цо)n} \le \tau_{\max n}; \\ 0, \textit{ при } \tau_{(цо)n} > \tau_{\max n}, \end{cases} \tag{4}$$

$\tau_{(цо)n}$ – время реализации n-го, $n = 1, 2, \ldots, N$, цикла обработки информации в КС;

$\tau_{\max n}$ – максимально допустимое значение величины $\tau_{(цо)n}$;

N – число циклов обработки информации, реализуемых в КС на временном отрезке $[t_1, t_2]$ ее исследования.

Вероятность $P(\tau \le \tau_{\max})$ характеризует своевременность реализации информационных процессов в КС. Соответствующий этой величине показатель E определяет возможности КС по реализации своей целевой функции – функции информационного обеспечения предметной деятельности в условиях воздействия ВПО и мер антивирусной защиты:

$$E = P(\tau \le \tau_{\max}). \tag{5}$$

Своевременность реагирования на воздействия ВПО средствами антивирусной защиты в КС характеризуются нормированным показателем времени обнаружения и блокирования ВПО данными средствами [15]. При этом, нормирование проводится относительно продолжительности воздействия ВПО. Формально это можно представить условиями:

$$\tau_{(аз)} \le \tau_{(ВПО)} \tag{6}$$

и

$$\tau_{(аз)} > \tau_{(ВПО)}, \tag{7}$$

где $\tau_{(аз)}$ и $\tau_{(ВПО)}$ – время реализации антивирусными средствами функций обнаружения и блокирования ВПО и продолжительность воздействия ВПО, соответственно.

В общем случае обе входящие в неравенства (6) и (7) величины являются случайными, поэтому его выполнение является случайным событием. Вероятность $P(\tau_{(аз)} \le \tau_{(ВПО)})$ этого события представляет собой среднее количество ситуаций, в которых ВПО было своевременно обнаружено и блокировано средствами антивирусной защиты

относительно общего числа зафиксированных воздействий ВПО на временном отрезке $[t_1, t_2]$ исследования:

$$P\left(\tau_{(аз)} \le \tau_{(ВПО)}\right) = \frac{1}{K} \cdot \sum_{k=1}^{K} \beta_k \,, \tag{8}$$

где $$\beta_k = \begin{cases} 1, \textit{ при } \tau_{(аз)k} \le \tau_{(ВПО)k}; \\ 0, \textit{ при } \tau_{(аз)k} > \tau_{(ВПО)k}, \end{cases} \tag{9}$$

$\tau_{(аз)k}$ – время обнаружения и блокирования ВПО антивирусными средствами КС при реализации k-го, $k = 1, 2, \ldots, K$, воздействия;

$\tau_{(ВПО)k}$ – продолжительность k-го, $k = 1, 2, \ldots, K$, воздействия ВПО;

K – число воздействий ВПО на временном отрезке $[t_1, t_2]$.

Вероятность $P(\tau_{(аз)} \le \tau_{(ВПО)})$ характеризует своевременность реагирования на воздействия ВПО в КС и рассматривается как показатель D возможностей средств антивирусных средств:

$$D = P(\tau_{(аз)} \le \tau_{(ВПО)}). \tag{10}$$

С целью формального доказательства гипотезы предположим, что продолжительности циклов обработки информации в КС равны между собой:

$$\tau_{(цо)} = \tau_{(цо)1} = \tau_{(цо)2} = \ldots = \tau_{(цо)n} = \ldots = \tau_{(цо)N}, \tag{11}$$

В этом случае величину времени τ реализации информационных процессов в КС представим в виде:

$$\tau = N \cdot \tau_{(цо)} + \tau_{(аз)}, \tag{12}$$

где $\tau_{(аз)}$ – время реализации процедур антивирусной защиты (соответствует условию (6));

N – количество циклов обработки информации, выполняемых за время τ.

Так как угроза воздействия ВПО может проявиться в любой точке отрезка $[t_1, t_2]$ продолжительность угрозы $\tau_{(ВПО)}$ определим как:

$$\tau_{(ВПО)} = N \cdot \tau_{(цо)}. \tag{13}$$

На основании выражения (6) определим в качестве условия своевременного реагирования на угрозу воздействия ВПО средствами антивирусной защиты следующее неравенство:

$$\tau_{(аз)} \le N \cdot \tau_{(цо)}, \tag{14}$$

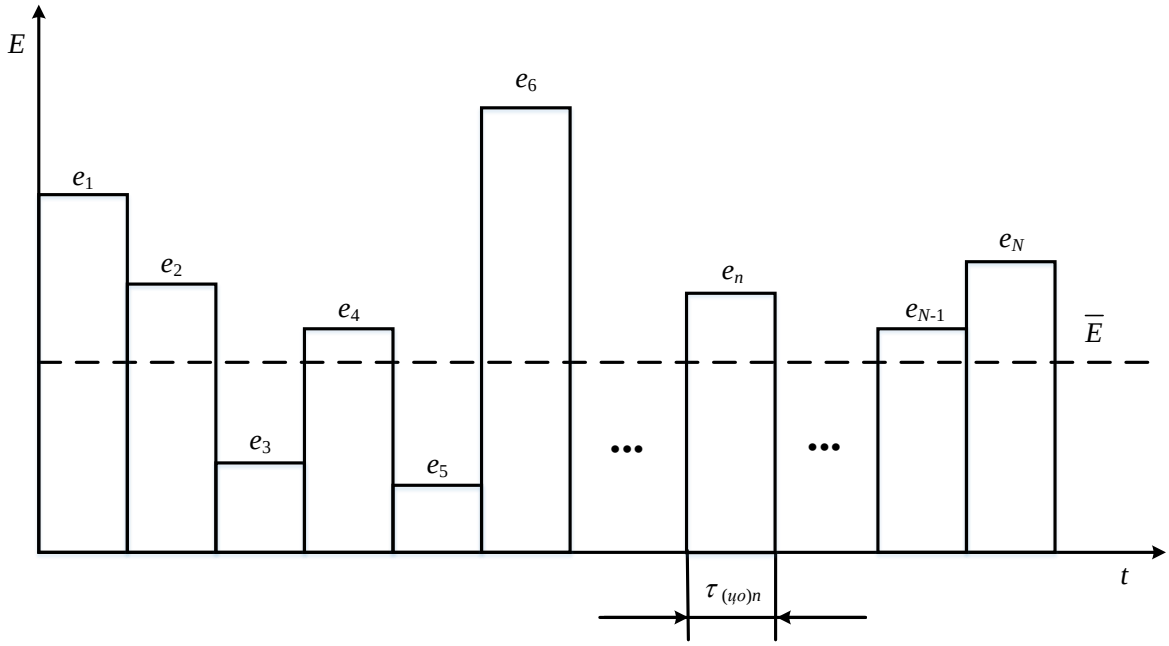
левая часть которого соответствует времени обнаружения и блокирования ВПО антивирусными средствами КС, а правая – времени существования угрозы воздействия ВПО.

Представим выражение для среднего значения показателя (5) в виде:

$$\bar{E} = \frac{\sum_{n=1}^{N} e_n}{N}, \tag{15}$$

где e_n – характеризует своевременность реализации информационного процесса в КС во время n-го цикла обработки информации (рис. 1):

$$e_n = P(\tau_{(цо)n} \le \tau_{\max n}). \tag{16}$$



Условные обозначения:
e_n – своевременность реализации информационного процесса в КС во время n-го цикла обработки информации;
$\tau_{(цо)n}$ – продолжительность n-го цикла обработки информации.

Рис. 1. Иллюстрация динамики изменения своевременности реализации информационных процессов в КС в различных циклах обработки информации
Fig. 1. Illustration of the dynamics of changes in the efficiency of information support of the CS in the process of implementing information processing cycles

В выражении (16) переменная $\tau_{\max n}$ соответствует (3).

Путем обратного преобразования из выражения (16) получим выражение для $\tau_{(цо)n}$:

$$\tau_{(цо)n} = f_1^{-1}(e_n), \quad (17)$$

где $f_1^{-1}(x)$ – функция обратная $P(y)$.

Воспользовавшись выражением (17) условие (14) представим в виде:

$$\tau_{(аз)} \le N \cdot f^{-1}(\bar{E}), \quad (18)$$

а выражение (10) – в виде:

$$D = P(\tau_{(аз)} \le N \cdot f^{-1}(\bar{E})). \quad (19)$$

Из выражения (19) следует, что существует соответствие значений характеристики своевременности реагирования на воздействия ВПО средствами антивирусной защиты значениям характеристики своевременности реализации информационных процессов в КС. Что и требовалось доказать.

3. Гипотеза об адекватности характеристик мер антивирусной защиты характеристикам угрозы воздействия ВПО

Формулировка гипотезы: существует соответствие между значением вероятности угрозы воздействия ВПО и значением характеристики своевременности реагирования на такого рода воздействие средствами антивирусной защиты.

С целью доказательства гипотезы дадим формальную интерпретацию характеристики возможностей нарушителя по несанкционированному доступу (НСД) к компьютерной информации с использованием ВПО, как способа деструктивного воздействия на информацию КС. С этой целью, по аналогии с [16], воспользуемся описательным характером базовой модели угроз безопасности информации и введем ряд уточнений данной модели, учитывающих особенности действий нарушителя при использовании ВПО в качестве инструмента реализации угрозы [17]. Естественно ожидать, что на содержание данной модели оказывает существенное влияние специфика применяемых мер антивирусной защиты.

Суть уточнений сводится к созданию предпосылок для обоснованного использования известных математических абстракций при формализованном представлении угрозы воздействия ВПО на КС. В общем случае такого рода уточнения сводятся к следующему:

1) нарушитель безопасности информации в КС может быть квалифицирован как внутренним, так и внешним нарушителем. При этом их возможности по внедрению ВПО и управлению выполнением им своих функций одинаковы;

2) нарушение безопасности информации в КС при использовании ВПО в качестве инструмента реализации угрозы ее безопасности связано с несанкционированным копированием, модификацией информации в этих системах, а также блокированию доступа к их информационным ресурсам. Действия нарушителя при этом жестко регламентированы способами применения ВПО и их характеристиками [18];

3) кратность действий нарушителя по внедрению ВПО и управлению выполнением им своих функций существенно ограничена из соображений обеспечения скрытности своих действий [18];

4) следствием ограниченности действий нарушителя является возможность ВПО самостоятельно (без вмешательства нарушителя) реализовывать свои функции в соответствии с алгоритмом функционирования [19];

5) как правило, в соответствии с требованиями обеспечения живучести ВПО, оно проектируется таким образом, что процесс выполнения им отдельных функций осуществляется дискретно, таким образом, что после выполнения очередной функции вредоносная программа, для маскирования своего присутствия в операционной среде КС, делает паузу в работе [19];

6) применение антивирусных средств не гарантирует стопроцентную вероятность обнаружения воздействий ВПО, кроме того, даже в случае обнаружения не гарантировано своевременное блокирование ВПО.

Рассмотренные уточнения позволяют представить процесс реализации угрозы НСД к компьютерной информации с использованием ВПО как последовательность соответствующих событий, связанных с действиями нарушителя, на временном отрезке $[t_1, t_2]$ от момента времени t_1 начала до момента t_2 окончания исследования. С целью обоснования возможности использования известной математической абстракции – закона Пуассона [13] при формализованном представлении последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, определим, характерны ли такой последовательности свойства стационарности, ординарности и отсутствия последействия?

С целью проверки предположения о стационарности последовательности событий, связанных с воздействием ВПО на информацию в КС, соотнесем длину временного отрезка $\tau_{(u)} = t_2 - t_1$ исследования с периодичностью $T_{(ВПО)}$ проявления такого воздействия и с его продолжительностью $\tau_{(ВПО)}$ (см. выражение (13)).

Стационарность последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, обусловлена следующими соотношениями между продолжительностью $\tau_{(u)}$ исследования угрозы и ее временными параметрами – средними значениями случайных величин $T_{(ВПО)}$ и $\tau_{(ВПО)}$:

$$\tau_{(u)} > \overline{T}_{(ВПО)}, \tag{20}$$

$$\tau_{(u)} >> \overline{\tau}_{(ВПО)}, \tag{21}$$

где $\overline{T}_{(ВПО)}$ и $\overline{\tau}_{(ВПО)}$ – средние значения случайных величин $T_{(ВПО)}$ и $\tau_{(ВПО)}$, соответственно.

Исходя из этого следует предположить, что моменты начала выполнения ВПО своих функций в процессе реализации угрозы имеют одинаковую среднюю плотность $\overline{\lambda}_{(ВПО)}$, которая не меняется во времени, а зависит лишь от периода $T_{(ВПО)}$:

$$\overline{\lambda}_{(ВПО)} = \frac{1}{\overline{T}_{(ВПО)}}. \tag{22}$$

Это, в свою очередь, характеризует однородность потока подобного рода событий во времени, из чего следует, что вероятность $P_{(ВПО)}$ воздействия ВПО определяется лишь длиной временного отрезка $\tau_{(u)}$ исследования и не зависит от положения данного отрезка на временной оси. Отсюда будет справедливым утверждение:

для произвольных $\tau_{(u)1}$ и $\tau_{(u)2}$, связанных неравенством $\tau_{(u)1} > \tau_{(u)2}$, будет справедливым соотношение: $P_{(ВПО)}(\tau_{(u)1}) > P_{(ВПО)}(\tau_{(u)2})$ при $\overline{\lambda}_{(ВПО)} = \text{Const}$.

Обоснованием свойства ординарности у последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, служит дискретный характер процесса выполнения им своих функций.

Доказательство свойства отсутствия последействия у последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, основывается на том, что свои функции ВПО реализует в последовательные моменты времени независимо друг от друга в соответствии с алгоритмом работы.

Наличие свойств стационарности, ординарности и отсутствия последействия у последовательности случайных событий, связанных с реализацией угрозы воздействия ВПО на КС, позволяет случайный характер таких воздействий описать законом Пуассона. В этом случае вероятность $P_{(ВПО)}$ хотя бы одного воздействия ВПО распределяется по экспоненциальному закону:

$$P_{(ВПО)} = 1 - e^{-\frac{\tau_{(u)}}{\overline{T}_{(ВПО)}}}. \tag{23}$$

Путем обратного преобразования из (23) получим выражение для $\tau_{(u)}$:

$$\tau_{(u)} = f_2^{-1}(P_{(ВПО)}), \tag{24}$$

где $f_2^{-1}(z)$ – функция обратная $P(u)$.

Воспользовавшись выдвинутым при доказательстве гипотезы 1 предположением о том, что угроза воздействия ВПО может проявиться в любой точке на отрезке $[t_1, t_2]$ выражение (10) запишем в виде:

$$D = P(\tau_{(аз)} \le f_2^{-1}(P_{(ВПО)})). \tag{25}$$

Из выражения (25) следует, что существует соответствие значений характеристики своевременности реагирования на воздействия ВПО средствами антивирусной защиты значениям вероятности такого воздействия. Что и требовалось доказать.

Заключение

Рассмотренные гипотезы и их доказательства могут служить теоретическим основанием для решения ряда задач, связанных с обоснованием таких значений временных параметров средств антивирусной защиты, которые соответствовали бы требуемым значениям характеристики своевременности реализации информационных процессов в КС и реальным значениям вероятности угрозы воздействия ВПО. Кроме того, предложенный вариант формального представления характеристик для оценки возможностей по своевременной реализации информационных процессов в КС, возможностей нарушителя по реализации НСД к компьютерной информации с использованием ВПО и возможностей по своевременному реагированию на воздействия ВПО антивирусными средствами может быть использован при построении математических моделей для такой оценки. Для этого достаточно использовать сходство выражений (5), (10), (19) и (25) с функцией распределения вероятностей и оценить законы распределения случайных величин, входящих в эти выражения. Это позволяет получить аналитические выражения (модели) соответствующих характеристик и количественно оценить возможности антивирусных средств.

СПИСОК ЛИТЕРАТУРЫ:

1. Зегжда Д.П., Александрова Е.Б., Калинин М.О. и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия – Телеком. 2020. – 560 с. URL: https://www.elibrary.ru/item.asp?id=48098225&ysclid=lboz6m45fc564834926 (дата обращения: 23.09.2022). – EDN: BLBTDA.
2. Киселев В.В., Голубков Д.А., Арутюнова В.И. Классификационная характеристика угроз воздействия вредоносных программ на информационные процессы в компьютерных системах. Вестник Воронежского института ФСИН России. 2016, № 2, с. 49–56. URL: https://www.elibrary.ru/item.asp?id=26673446&ysclid=lboxxsw19s896355802 (дата обращения: 03.11.2022). – EDN: WLSBPR.
3. Холмогоров В. Pro Вирусы: Издание третье, переработанное и дополненное. СПб.: ООО «Страта». 2018. – 162 с. URL: http://www.bibliorossica.com/book.html?currBookId=33644 (дата обращения: 27.11.2022).
4. Монаппа К.А. Анализ вредоносных программ. М.: Издательство «ДМК Пресс», 2018. – 452 с. URL: https://coollib.net/b/592264-k-a-monappa-analiz-vredonosnyih-programm/read?ysclid=lbw6j1ik3975436353 (дата обращения: 03.11.2022).
5. Томас Дж. Холт, Адам М. Босслер, Кэтрин К. Сейгфрид-Спеллар. Киберпреступность и цифровая криминалистика: Введение. Лондон и Нью–Йорк: Ратледж, 2015. – 485 с.
6. Савицкий А. Опрос: Самая непонятная киберугроза. Лаборатория Касперского (10 февраля 2014). URL: https://www.kaspersky.ru/blog/opros-samaya-neponyatnaya-kiberugroza/2960/ (дата обращения: 03.11.2022).
7. Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки. М.: ФОРУМ: ИНФРА-М, 2007. – 528 с.
8. Скрыль С.В., Сычев М.П., Бардаев Э.А., Хворов Р.А., Голубков Д.А. Оптимизация процесса обеспечения антивирусной защиты в автоматизированных системах управления специального назначения. Телекоммуникации. 2016, № 3, с. 21–27. URL: https://www.elibrary.ru/item.asp?id=25675664&ysclid=lboy6qvj91608910531 (дата обращения: 27.11.2022). – EDN: VPWJNJ.
9. Скрыль С.В., Сычев А.М., Мещерякова Т.В., Арутюнова В.И., Голубков Д.А. Оценка защищенности информации от вирусных атак: существующий и перспективный методический аппарат. Промышленные АСУ и контроллеры. 2018, № 9, с. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304&ysclid=lboygrexgr402942258 (дата обращения: 27.11.2022). – EDN: YABXKX.
10. Вайц Е.В., Сычев В.М. Методика оценки угроз безопасности информации ФСТЭК России как концепция исследования вопросов обеспечения безопасности объектов инфокоммуникационной инфраструктуры электронной коммерции. Вопросы защиты информации. 2021, № 4, с. 50–58. URL: http://izdat.ntckompas.ru/news/detail.php?ID=27015 (дата обращения: 27.11.2022).
11. Сычев М.П., Гайфулин В.В., Вайц Е.В., Скрыль К.С., Хворов Р.А. Методика оценки угроз безопасности

информации» ФСТЭК России как инструмент исследования компьютерных атак на информационные ресурсы автоматизированных систем управления специального назначения. Приборы и системы. Управление, контроль, диагностика. 2022, № 1, с. 27–32. DOI: http://dx.doi.org/10.25791/pribor.1.2022.1316. – EDN: VSXHDP.

12. Мещерякова Т.В., Сычев А.М., Арутюнова В.И. Формализованное описание вирусных атак на информационные ресурсы центров обработки данных и механизмов антивирусной защиты. Охрана, безопасность, связь. Воронеж: Воронежский институт МВД России. 2019, с. 109–114. URL: https://www.elibrary.ru/item.asp?id=32839477&ysclid=lboyw9o8i2194258210 (дата обращения: 27.11.2022). – EDN: YWTVZG.
13. Мещерякова Т.В., Скрыль К.С., Вайц Е.В., Гайфулин В.В., Грачева Ю.В. Классические математические абстракции в приложениях теории информационной безопасности. Приборы и системы. Управление, контроль, диагностика. 2022, № 1, с. 37–46. DOI: http://dx.doi.org/10.25791/pribor.1.2022.1318. – EDN: AOIRTY.
14. Зыбин Д.Г., Голубков Д.А., Арутюнова В.И. Показатели эффективности информационных процессов в компьютерных системах в условиях защиты информации от вредоносных программ. Вестник Воронежского института ФСИН России. 2016, № 2, с. 40–49. URL: https://www.elibrary.ru/item.asp?id=26673445&ysclid=lbozsqw3rx608640161 (дата обращения: 27.11.2022). – EDN: WLSBPH.
15. Скрыль С.В., Сычев А.М., Громов Ю.Ю., Мещерякова Т.В., Арутюнова В.И. Определение показателя своевременности реагирования на угрозы безопасности компьютерной информации. Промышленные АСУ и контроллеры. 2016, № 5, с. 59–64. URL: http://asu.tgizd.ru/ru/arhiv/15201 (дата обращения: 27.11.2022).
16. Сычев М.П., Гайфулин В.В., Сычев В.М., Вайц Е.В., Абачараева Э.Р. Киберустойчивость информационной инфраструктуры: модели исследования: монография. М.: Русайнс, 2021. – 254 с. URL: https://book.ru/book/942052 (дата обращения: 27.11.2022).
17. Мещерякова Т.В., Арутюнова В.И. Модель нарушения безопасности информации с применением вредоносных программ. Охрана, безопасность и связь. Воронеж: Воронежский институт МВД России. 2017, с. 80–84. URL: https://www.elibrary.ru/item.asp?id=28920559&ysclid=lbw527vqgw429655263 (дата обращения: 12.10.2022). – EDN: YIWOXX.
18. Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом. Хрестоматия. М.: Норма, 2022. – 528 с. URL: https://bik.sfu-kras.ru/elib/view?id=LANY-44.03.05/%D0%9E-356-617617911&ysclid=lbw54e5yhn317125773 (дата обращения: 12.10.2022).
19. Голубков Д.А., Жучков Р.Э. Характеристика противоправных действий, совершаемых с использованием вредоносных программ. Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: Материалы Всероссийской научно-практической конференции. Воронеж: Воронежский институт МВД России. 2014, с. 121–123. ISBN 978-5-88591-175-7.

REFERENCES:

[1] Zegzhda D.P., Alexandrova E.B., Kalinin M.O., etc. Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks. M.: Hotline – Telecom. 2020. – 560 p. URL: https://www.elibrary.ru/item.asp?id=48098225&ysclid=lboz6m45fc564834926 (accessed: 23.09.2022) (in Russian). – EDN: BLBTDA.
[2] Kiselev V.V., Golubkov D.A., Arutyunova V.I. Classification risk characterization exposure malware on information processes in the data center. Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2016, no. 2, p. 49–56. URL: https://www.elibrary.ru/item.asp?id=26673446&ysclid=lboxxsw19s896355802 (accessed: 03.11.2022) (in Russian). – EDN: WLSBPR.
[3] Kholmogorov V. Pro Viruses: Third edition, revised and supplemented. St. Petersburg: LLC "Strata". 2018. – 162 p. URL: http://www.bibliorossica.com/book.html?currBookId=33644 (accessed: 27.11.2022) (in Russian).
[4] Monappa K.A. Malware analysis. M.: DMK Press Publishing House. 2018. – 452 p. URL: https://coollib.net/b/592264-k-a-monappa-analiz-vredonosnyih-programm/read?ysclid=lbw6j1ik3975436353 (accessed: 03.11.2022) (in Russian).
[5] Thomas J Holt, Adam M Bossler, Kathryn C Seigfried-Spellar. Cybercrime and Digital Forensics: An Introduction. London and New York: Routledge, 2015. – 485 p.
[6] Savitsky A. Poll: The most incomprehensible cyber threat. Kaspersky Lab (February 10, 2014). URL: https://www.kaspersky.ru/blog/opros-samaya-neponyatnaya-kiberugroza/2960/ (accessed: 03.11.2022).

[7] Partyka T.L., Popov I.I. Operating systems, environments and shells. M.: FORUM: INFRA-M, 2007. – 528 p.
[8] Skryl S.V., Sychev M.P., Bardayev E.A., Khvorov R.A., Golubkov D.A Support process optimization of antivirus protection in automated control systems of special purpose. Telecommunications. 2016, no. 3, p. 21–27. URL: https://www.elibrary.ru/item.asp?id=25675664&ysclid=lboy6qvj91608910531 (accessed: 27.11.2022) (in Russian).
[9] Skryl S.V., Sychev A.M., Meshcheryakova T.V., Arutyunova V.I., Golubkov D.A. Evaluation of information security from virus attacks: existing and future methodological apparatus. Industrial automated control systems and controllers. 2018, no. 9, p. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304&ysclid=lboygrexgr402942258 (accessed: 27.11.2022) (in Russian).
[10] Vayts E.V., Sychev V.M. Methodology for assessing threats to information security of the FSTEC of Russia as a concept for researching issues of ensuring the security of objects of the infocommunication infrastructure of e-commerce. Information Security Issues. 2021, no. 4, p. 50–58. URL: http://izdat.ntckompas.ru/news/detail.php?ID=27015 (accessed: 27.11.2022) (in Russian).
[11] Sychev M.P., Gayfulin V.V., Vaits E.V., Skryl K.S., Khvorov R.A. Methodology for assessing information security threats FSTEC of Russia as a tool for studying computer attacks on information resources of automated control systems for special purposes. Devices and Systems. Management, control, diagnostics. 2022, no. 1, p. 27–32. DOI: http://dx.doi.org/10.25791/pribor.1.2022.1316 (in Russian). – EDN: VSXHDP.
[12] Meshcheryakova T.V., Sychev A.M., Arutyunova V.I. Formalized description of virus attacks on information resources of data centers and mechanisms of antivirus protection. Security, safety, communication. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2018, p. 109–114. URL: https://www.elibrary.ru/item.asp?id=32839477&ysclid=lboyw9o8i2194258210 (accessed: 27.11.2022) (in Russian). – EDN: YWTVZG.
[13] Meshcheryakova T.V., Skryl K.S., Vayts E.V., Gayfulin V.V., Gracheva Yu.V. Classical mathematica abstractions in applications of notitia securitatem theoria. Devices and systems. Management, control, diagnostics. 2022, no. 1, p. 37–46. DOI: http://dx.doi.org/10.25791/pribor.1.2022.1318 (in Russian). – EDN: AOIRTY.
[14] Zybin D.G., Golubkov D.A., Arutyunova V.I. Efficiency indexes of information processes in computer systems under conditions of protecting information from malicious software. Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2016, no. 2, p. 40–49. URL: https://www.elibrary.ru/item.asp?id=26673445&ysclid=lbozsqw3rx608640161 (accessed: 27.11.2022) (in Russian). – EDN: WLSBPH.
[15] Skryl S.V., Sychev A.M., Gromov Yu.Yu., Meshcheryakova T.V., Arutyunova V.I. Determination of the indicator of timely response to threats to the security of computer information. Industrial automated control systems and controllers. 2016, no. 5, p. 59–64. URL: http://asu.tgizd.ru/ru/arhiv/15201 (accessed: 27.11.2022) (in Russian).
[16] Sychev M.P., Gayfulin V.V., Sychev V.M., Weiss E.V., Abacharaeva E.R. Cyber stability of information infrastructure: research models: monograph. M.: Rusains, 2021. – 254 p. URL: https://book.ru/book/942052. (accessed: 27.11.2022) (in Russian).
[17] Meshcheryakova T.V., Arutyunova V.I. Model of violation of safety of information with application of malicious applications. Security, safety and communication. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2017, p. 80–84. URL: https://www.elibrary.ru/item.asp?id=28920559&ysclid=lbw527vqgw429655263 (accessed: 12.10.2022) (in Russian). – EDN: YIWOXX.
[18] Ovchinsky V.S. Fundamentals of the fight against cybercrime and cyberterrorism. Textbook. M.: Norm, 2017. – 528 p. URL: https://bik.sfu-kras.ru/elib/view?id=LANY-44.03.05/%D0%9E-356-617617911&ysclid=lbw54e5yhn317125773 (accessed: 12.10.2022) (in Russian).
[19] Golubkov D.A., Zhuchkov R.E. Characteristics of illegal actions committed with the use of malicious programs. Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes: Materials of the All-Russian Scientific and practical Conference. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2014, p. 121–123. ISBN 978-5-88591-175-7 (in Russian).

Поступила в редакцию – 05 декабря 2022 г. Окончательный вариант – 01 февраля 2023 г.
Received – December 05,2022. The final version – February 01, 2023.