УДК 004.942

Построение инструментальной модели для исследования системы "Компьютерный вирус–переносчик–автоматизированное рабочее место–локальная вычислительная сеть"

С. Н. Горячев, Н. С. Кобяков, С. Н. Костарев
Пермский военный институт войск национальной гвардии Российской Федерации
Россия, 614030, г. Пермь, ул. Гремячий Лог, 1
sergory@mail.ru; kkobyakov1234@gmail.com;
+79194682073; +79222440454

Рассмотрен механизм заражения компьютерными вирусами автоматизированных рабочих мест, передача вируса от зараженного автоматизированного рабочего места к незараженному. Проанализировано воздействие компьютерного вируса на локально-вычислительную сеть. Представлена инструментальная модель для исследования системы "Компьютерный вирус–переносчик–автоматизированное рабочее место–локальная вычислительная сеть".

Ключевые слова: *компьютерные вирусы; инструментальная модель; автоматизированное рабочее место; передача компьютерных вирусов.*

DOI: 10.17072/1993-0550-2021-1-53-56

Введение

В век широкого развития информационных технологий и повсеместного их применения все большие обороты набирает создание не только программного обеспечения, для выполнения прикладных задач, но и также программного обеспечения, предназначенного для деструктивного воздействия на отдельные автоматизированные рабочие места (АРМ) и в целом локальная вычислительную сеть (ЛВС). Компьютерный вирус – это программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия [1]. При этом копии сохраняют способность дальнейшего распространения [1].

Компьютерный вирус относится к категории вредоносных программ.

На рис. 1 представлена статистика заражения компьютерными вирусами в апреле-июне 2020 года на основании отчета лаборатории Касперского [2].

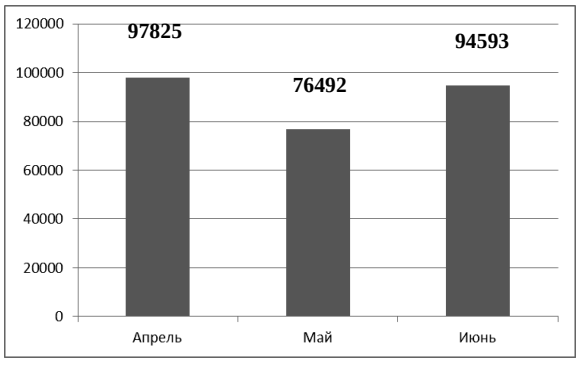

Рис. 1. *Статистика заражения компьютерными вирусами персональных компьютеров в апреле-июне 2020 года* [2]

1. Материалы и методы исследования

Проблеме борьбы с компьютерными вирусами уже более 30 лет и работы, проводимые по исследованию данной проблемы, можно разделить на два направления:

1. Применение общей теории систем, системного анализа и прикладных исследований [2–4].
2. Исследование прогнозных моделей развития компьютерных вирусов [5–7].

При разработке инструментальной модели использовалась общая теория систем, статистический анализ, дифференциально-интегральное исчисление, теория множеств и графов.

2. Результаты исследования и их обсуждение

2.1. Построение графа модели состояний и переходов системы

Предлагаемые модели представлены 4 элементами: (*L*) – ЛВС, состоящая из передающей среды (кабелей), рабочих станций (автоматизированных рабочих мест), имеющая следующие характеристики: скорость передачи данных, задержка распространения сигналов, защищенность и надежность передачи. (CV) – источники компьютерных вирусов (*V*) – переносчики (зараженные) файлы, объединенные в сеть элементами представленной системы и (*Ar*) – незараженное АРМ, на которое взаимосвязанно действуют все элементы системы.

В представленной системе важную роль играет процесс передачи компьютерного вируса от зараженного АРМ к незараженному. АРМ от компьютерного вируса защищает два поля: 1 – антивирусная защита (программа), 2 – защита от несанкционированного доступа (программно-аппаратные средства от НСД). Для размножения компьютерного вируса необходим сам компьютерный вирус (CV), переносчик (*V*) и автоматизированное рабочее место (*Ar*).

На компьютерный вирус также оказывает состояние локально-вычислительной сети (CV-L-V-Ar). Граф состояний и переходов системы "CV-L-V-Ar" показан на рис. 2.

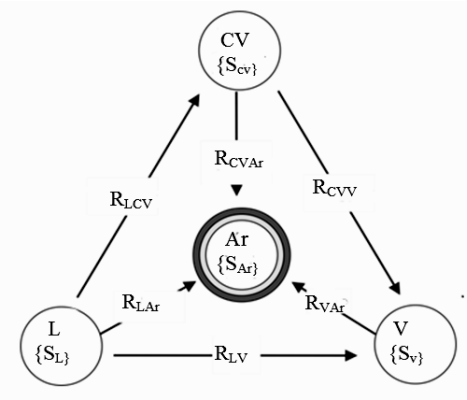

Рис. 2. *Граф состояний и переходов системы "CV-L-V-Ar"*

2.1.1. Определение состояния системы

При идентификации системы CV-L-V-Ar введем определение состояния безопасности системы. Рассмотрим систему CV-L-V-Ar как систему, осуществляющую отображение семейства множеств $H(t)$ на множество Z, т.е. $ZRH(t)$. Задача синтеза системы может заключаться в определении множества входных временных сигналов. Разложим R на бинарные множества R^1 и R^2:

$$Z\ R^1\left[H(t), C\right],\ CR^2H(t). \qquad (1)$$

Элементы С описывают состояние (память) системы. Разложение системы на два множества показывает, что Z не зависит от предыстории состояния системы, т.е. будет формализовываться полумарковским процессом. В качестве входов и выходов системы выбираются элементы системы, доступные для мониторинга и измерения заражения компьютерными вирусами.

В данной статье проведено исследование критичных состояний системы CV-L-V-Ar: безопасного и опасного при учете взаимного влияния элементов системы.

2.1.2. Построение детерминированной модели оценки состояния системы

Состояние безопасности АРМ C_{Ar} зависит от его собственных свойств S_{Ar} – установленной антивирусной программы и средств защиты от несанкционированного доступа:

$$C_{Ar}= \Phi_1[\{S_{Ar}\}, C_{Ar}^{CV}, C_{Ar}^{L}, C_{Ar}^{V}]. \qquad (2)$$

Состояние зараженного АРМ C_V зависит от собственных свойств переносчика – S_V – количество узлов сети, к которым он подключен и от состояния ЛВС (L) и состояния вируса (CV):

$$C_V = \Phi_3[\{S_V\}, C_V^{CV}, C_V^{L}]. \quad (3)$$

Состояние компьютерного вируса зависит от собственных свойств компьютерного вируса S_{CV} и влияния характеристик ЛВС на скорость распространения вируса

$$C_{CV} = F_4[\{S_{CV}\}, C_{CV}^{L}]. \quad (4)$$

Таким образом, модель оценки состояния системы ЛВС "CV-L-V-Ar" опишется функцией

$$C_{CV\text{-}L\text{-}V\text{-}Ar} = \Psi[C_{Ar}, C_V, C_L, C_{CV}]. \quad (5)$$

2.2. Исследование безопасности состояния системы

2.2.1. Исследование состояния системы защиты незараженного

Изменение состояния автоматизированного рабочего места (*Ar*) опишется зависимостью

$$C_{Ar} = \Delta M(S)+\Delta M(CV)+\Delta M(L)+\Delta M(V), \quad (6)$$

где $\Delta M(S)$ – изменение состояния АРМ от собственных свойств, $\Delta M(CV)$ – изменение состояния АРМ от воздействия компьютерного вируса, $\Delta M(L)$ – изменение состояния АРМ от характеристики ЛВС, $\Delta M(V)$ – изменение состояния АРМ от внедрения переносчика.

Под индивидуальными свойствами безопасности АРМ можно понимать наличие антивирусной защиты (*Az*), использование средств защиты от НСД (*Zn*):

$$\Delta M\ (S) = \frac{\partial M}{\partial S_{Az}} \Delta S_{Az} + \frac{\partial M}{\partial S_{Zn}} \Delta S_{Zn}. \quad (7)$$

От характеристики ЛВС сильно зависит скорость распространения компьютерного вируса, например пропускной способности (*Pr*), скорости передачи данных (*Sp*):

$$\Delta M\ (L) = \frac{\partial M}{\partial L_{\mathrm{Pr}}} \Delta L_{\mathrm{Pr}} + \frac{\partial M}{\partial L_{Sp}} \Delta L_{Sp}. \quad (8)$$

Внедрение в АРМ переносчика с компьютерным вирусом является важным элементом при заражении АРМ, например, отсутствие или несвоевременное обновление сигнатур антивирусных баз $\{V_1\}$, несанкционированное подключение съемного носителя $\{V_2\}$, письма с вирусными вложениями на электронную почту и др. $\{V_3\}$

$$\Delta M(V) = \frac{\partial M}{\partial V_1} \Delta V_1 + \frac{\partial M}{\partial V_2} \Delta V_2 + \frac{\partial M}{\partial V_3} \Delta V_3\ . \quad (9)$$

Вывод

На основе подходов системного анализа разработана детерминированная модель исследования состояний системы "Компьютерный вирус–переносчик–автоматизированное рабочее место–локально-вычислительная сеть" (CV-L-V-Ar) при изменении параметров системы.

Разработана методика оценки изменения состояния системы CV-L-V-Ar. Разработана модель информационной системы определения вредоности компьютерного вируса CV для поддержки принятия решений при оценке заражения ЛВС организации.

Список литературы

1. *ГОСТ Р* 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
2. URL:https://seCurelist.ru/it-threat-evolution-q2-2020-pC-statistiCs/98256/Развитие информационных угроз во втором квартале 2020 года. Статистика по ПК (дата обращения: 08.10.2020).
3. *Семыкина Н.А., Шавыкина И.В.* Математическая модель защиты компьютерной сети от вирусов // Программные продукты и системы. 2016. Вып. 116.
4. *Абидарова А.А*. Разновидности компьютерных вирусов // Достижения науки и образования. 2020. № 4.
5. *Булахов Н.Г.* Методы обнаружения компьютерных вирусов и сетевых червей // Доклады ТУСУР. 2008. № 1.

6. *Лесько С.А., Алешкин А.С., Филатов В.В.* Стохастические и перколяционные модели динамики блокировки вычислительных сетей при распространении эпидемий эволюционирующих компьютерных вирусов // Российский технологический журнал. 2019.

7. *Семенов С.Г., Давыдов В.В.* Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом // Вестник НТУ ХПИ. 2012. № 38.

Construction of an instrumental model for the study of the system "Computer virus–Carrier–automated workstation–local area network"

S. N. Goryachev, N. S. Kobyakov, S. N. Kostarev
Perm Military Institute of the National Guard Forces of the Russian Federation
1, Gremyachiy Log st., Perm, 614030, Russia
sergory@mail.ru, kkobyakov1234@gmail.com;
+79194682073; +79222440454

The mechanism of computer virus infection of workstations is considered, the transmission of a virus from an infected workstation to an uninfected one. The impact of a computer virus on a local area network is analyzed. An instrumental model for the study of the system "computer virus-carrier-automated workstation-local-computer network" is presented.

Keywords: *computer viruses; instrumental model; workstation; transmission of computer viruses.*