УДК 681.3

ВЕРОЯТНОСТНО-АНАЛИТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ ФАЙЛОВОГО ВИРУСА НА ЭЛЕМЕНТ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Н.М. Радько, Д.Н. Бочаров

В работе предлагается модель на основе сетей Петри-Маркова для описания процесса заражения элемента КС. Найдены вероятности: латентного инфицирования элемента, инфекционного заражения элемента, выхода из строя зараженного элемента, излечения элемента

Ключевые слова: сеть, вероятность, файл

С помощью сетей Петри-Маркова рассмотрим процесс заражения элемента компьютерной системы файловым вирусом [4]. В качестве элемента заражения возьмем файл операционной системы. Данный класс вирусов для реализации использует файлы операционной системы такие как: (динамические библиотеки DLL, драйвера SYS, приложения EXE) [3]. «Вредонос» меняет код заражаемого файла на свой. В результате зараженный элемент системы теряет свой исходный функционал [5].

Смоделируем поведение «вредоноса» с момента его отправки, до момента заражения элемента компьютерной системы. Для построения сети были использованы следующие термины:

S_1—злоумышленник готов к отправки вредоносного программного обеспечения,

S_2—устройство пользователя готово к приему вредоносного программного обеспечения,

t_1—определение способа отправки вредоносного программного обеспечения,

S_3—выбранный способ отправки вредоносного программного обеспечения,

t_2—настройка вредоносного программного обеспечения под выбранный тип отправки определяемы на шаге t_1,

S_4—вредоносное программного обеспечения готово к отправке,

S_5—выбранный способ отправки,

t_3—отправка вредоносного программного обеспечения на устройств,

S_6—вредоносное программного обеспечения находится на устройстве,

t_4—анализ системы на предмет возможного варианта запуска вредоносного программного обеспечения,

S_7—найденные возможности запуска вредоносного программного обеспечения (в данном случае два: по средствам автозапуска, по средствам запуска вредоносного программного обеспечения пользователем),

t_5—вредоносное программное обеспечения начинает работать в 2 потока (в данном случае это обеспечит большую вероятность запуска вредоносного кода),

S_8—первый поток направленный на обеспечение запуска вредоносного программного обеспечения через автозапуск,

S_9—второй поток, в котором запуск вредоносного программного обеспечения происходит по средствам пользователя,

t_6—правка реестра системы и добавление вредоносного программного обеспечения в автозагрузку,

S_{10}—вредоносное программное обеспечения ожидающее перезагрузку системы и последующий запуск,

t_7—запуск вредоносного программного обеспечения посредствам открытия приложения пользователем,

S_{11}—запущенное вредоносное приложение,

t_8—поиск подходящего к заражению объекта,

S_{12}—найденный и подходящий для заражения объект,

t_9—добавление вредоносного кода в найденный объект,

S_{13}—видоизмененный объект.

Граф данной сети представлен на рис. 1.

Радько Николай Михайлович –ВГТУ, доцент, канд. техн. наук, e-mail: mnac@comch.ru
Бочаров Дмитрий Николаевич – ВГТУ, студент, e-mail: d.bocharov@qip.ru

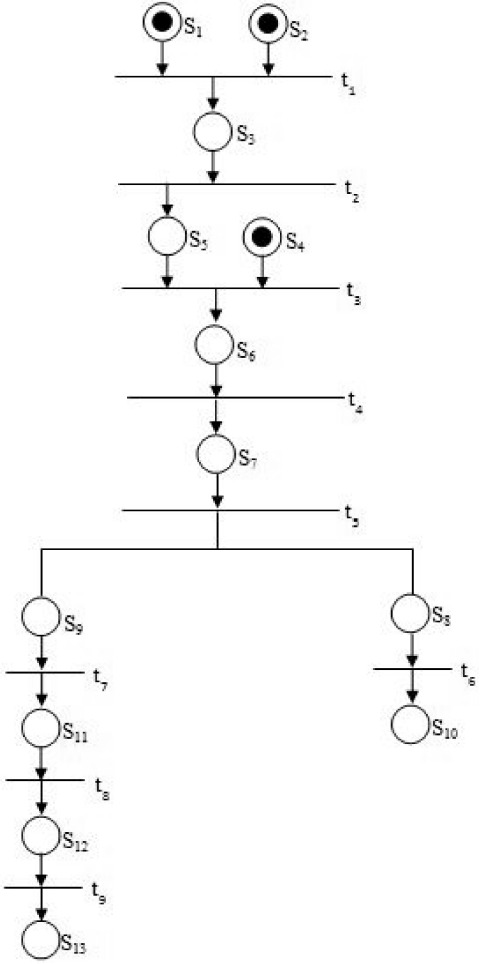

Рис. 1 Граф сети Петри-Маркова реализации атаки вредоносного ПО

Элементы матрицы, определяющие направленности дуг графа) следующим логические функции срабатывания сети, образом (1): могут быть записаны (без учета

Таблица 1

Матрица срабатывания сети

t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9
1	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0
$S_1t_1 \cap S_2t_1$	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0
0	0	$S_4t_3 \cap S_5t_3$	1	0	0	0	0	0
0	0	0	1	1	0	0	0	0
0	0	0	0	1	1	0	0	0
0	0	0	0	1	0	1	0	0
0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	1	0
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	1

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений (1):

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_{S_2t_1}(t) = \pi_{21}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_1(t) = \int_0^t f_{S_1t_1}(\tau)\,\Phi_{S_2t_1}(t) + f_{S_1t_1}(\tau)\Phi_{S_1t_1}(t),$$
$$\Phi_{S_3t_2}(t) = \pi_{32}\int_0^t f_{S_3t_2}(\tau)\Phi_1(t-\tau)d\tau,$$
$$\Phi_{S_4t_3}(t) = \pi_{43}\int_0^t f_{S_4t_3}(\tau)d\tau, \qquad (1)$$
$$\Phi_{S_5t_3}(t) = \pi_{53}\int_0^t f_{S_5t_3}(\tau)\Phi_1(t-\tau)d\tau,$$
$$\Phi_2(t) = \int_0^t f_{S_4t_3}(\tau)\,\Phi_{S_5t_3}(t) + f_{S_5t_3}(\tau)\Phi_{S_4t_3}(t),$$
$$\Phi_{S_6t_4}(t) = \pi_{64}\int_0^t f_{S_6t_4}(\tau)\Phi_2(t-\tau)d\tau,$$
$$\Phi_{S_7t_5}(t) = \pi_{75}\int_0^t f_{S_7t_5}(\tau)\Phi_{S_6t_4}(t-\tau)d\tau,$$
$$\Phi_{S_8t_6}(t) = \pi_{86}\int_0^t f_{S_8t_6}(\tau)\Phi_{S_7t_5}(t-\tau)d\tau,$$
$$\Phi_{S_9t_7}(t) = \pi_{97}\int_0^t f_{S_9t_7}(\tau)\Phi_{S_7t_5}(t-\tau)d\tau,$$
$$\Phi_{S_{11}t_8}(t) = \pi_{118}\int_0^t f_{S_{11}t_8}(\tau)\Phi_{S_9t_7}(t-\tau)d\tau,$$
$$\Phi_{S_{12}t_9}(t) = \pi_{129}\int_0^t f_{S_{12}t_9}(\tau)\Phi_{S_{11}t_8}(t--\tau)d\tau.$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид (2):

$$f_{S_it_j} = \alpha_{ij}e^{-\alpha_{ij}t}, \qquad (2)$$

где, $\alpha_{ij} = 1/\tau_{ij} i = 1,\ldots,13; j = 1,\ldots,9.$

Применение прямого и обратного преобразования Лапласа получается весьма громоздким, поэтому целесообразно применять пуассоновское приближение для плотностей распределения вероятностей времени перемещения в переходы сети Петри-Маркова.

Используя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения (3):

$$\tau_1 = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}},$$
$$\tau_2 = \tau_1 + \tau_{32},$$
$$\tau_3 = \tau_2 + \tau_{53},$$
$$\tau_4 = \frac{(\tau_2^2 + \tau_{53})^2 + (\tau_2 + \tau_{53})\tau_{43} + \tau_{43}^2}{(\tau_2 + \tau_{53}) + \tau_{43}}, \qquad (3)$$
$$\tau = \frac{(\frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^{2\,2}}{\tau_{11} + \tau_{21}}) + \tau_{32} + \tau_{53})^2 + (\frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}}) + \tau_{32} + \tau_{53})\tau_{43} + \tau_{43}^2}{(\frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}} + \tau_{32} + \tau_{53}) + \tau_{43}} + \tau_{64} + \tau_{75} + \tau_{86} + \tau_{97} + \tau_{118} + \tau_{129},$$

$$P(t) = 1 - e^{-\frac{1}{\tau}t},$$

где, исходные параметры атаки принимают следующие значения:

τ_{11} = - среднее время подготовки вредоносного программного обеспечения злоумышленником, τ_{21} = - среднее время подготовки устройства пользователя, τ_{32} = - - среднее время настройки вредоносного программного обеспечения под выбранный тип отправки, τ_{43} = - среднее время подготовки вредоносного программного обеспечения, τ_{53} = - среднее время отправки вредоносного программного обеспечения на устройств, τ_{64} = - среднее время анализа системы на предмет возможного варианта запуска вредоносного программного обеспечения, τ_{75} = - среднее время распоточивания вредоносного приложения, τ_{86} = - среднее время необходимое для

правки реестра системы и добавление вредоносного программного обеспечения в автозагрузку, τ_{97} = - среднее время необходимое для запуска вредоносного программного обеспечения, τ_{118} = - среднее время необходимое для поиска подходящего к заражению объекта, τ_{129} = - среднее время необходимое для добавление вредоносного кода в найденный объект, τ = - среднее время для всей цепи событий.

Из вышеприведенной сети Петри-Маркова можно найти t_0 - момент успеха атаки. Для данного типа вирусов $t_0 = t_3$, то есть времени отправки вредоносного программного обеспечения на устройство. Таким образом (4).

$$t_0 = \frac{\tau_2^2 + \tau_{43}\tau_2 + \tau_2^2}{\tau_{43} + \tau_2}. \qquad (4)$$

Вероятность инфекционного заражения элемента будет иметь вид (6):

$$P_{зи} = f(t_0)(\Delta t). \qquad (6)$$

Для перехода к плотности вероятности, необходимо взять производную от вероятности, полученной при помощи моделирования сетей Петри – Маркова (7).

$$f(t_0) = P'(t) = \left(1 - e^{-\frac{t_0}{\tau}}\right)' = \frac{e^{-\frac{t_0}{\tau}}}{\tau}, \qquad (7)$$

где t_0 – момент успеха атаки, τ – среднее время для всей цепочки событий, полученное при моделировании сетей Петри-Маркова.

Для нахождения Δt предположим, что функция является убывающей. Значит, максимальное значение она принимает в точке 0. Отсюда следует, что (8):

$$\Delta t = \frac{1}{n f_{\max}}.$$

$$f_{\max} = \frac{e^{-\frac{0}{\tau}}}{\tau} = \frac{1}{\tau},$$

$$\Delta t = \frac{1}{n f_{\max}} = \frac{1}{n\frac{1}{\tau}} = \frac{\tau}{n}, \qquad (8)$$

Тогда вероятность инфекционного заражения элемента будет равна (10):

$$P_{зи} = \frac{e^{-\frac{t_0}{\tau}}}{\tau}(\Delta t). \qquad (9)$$

Для нахождения вероятности излечения элемента необходимо смоделировать процесс лечения с помощью сети Петри-Маркова. Для построения сети были использованы следующие термины:

S_1—зараженный элемент компьютерной системы,

t_1—запуск антивирусного программного обеспечения,

S_2—антивирусное программное обеспечение,

t_2—подключение базы с сигнатурами вирусного программного обеспечения в антивирусе,

S_3—база с сигнатурами вредоносного программного обеспечения,

t_3—сравнение кода зараженного программного обеспечения с вирусной базой данных,

S_4—результат сравнения положительный,

t_4—поиск в зараженном элементе код вредоносного программного обеспечения,

S_5—найденный вредоносный код,

t_5—удаление вредоносного кода,

S_6—излеченный элемент.

Граф данной сети представлен на рис. 2

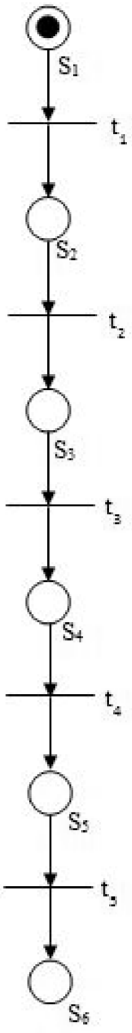

Рис. 2 Граф сети Петри-Маркова реализации излечения элемента компьютерной системы

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений (10):

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_{S_2t_2}(t) = \pi_{22}\int_0^t f_{S_2t_2}(\tau)\Phi_{S_1t_1}(t-\tau)d\tau,$$
$$\Phi_{S_3t_3}(t) = \pi_{33}\int_0^t f_{S_3t_3}(\tau)\Phi_{S_2t_2}(t-\tau)d\tau, \quad (10)$$
$$\Phi_{S_4t_4}(t) = \pi_{44}\int_0^t f_{S_4t_4}(\tau)\Phi_{S_3t_3}(t-\tau)d\tau,$$
$$\Phi_{S_5t_5}(t) = \pi_{55}\int_0^t f_{S_5t_5}(\tau)\Phi_{S_4t_4}(t-\tau)d\tau,$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид (11):

$$f_{S_it_j} = \alpha_{ij}e^{-\alpha_{ij}t}, \quad (11)$$

Где $\alpha_{ij} = 1/\tau_{ij} i = 1,\ldots,6; j = 1,\ldots,5.$

Используя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода(12).

$$\tau = \tau_{11} + \tau_{22} + \tau_{33} + \tau_{44} + \tau_{55}, \quad (12)$$

где, исходные параметры атаки принимают следующие значения:

τ_{11} - среднее время необходимое для запуска антивирусного программного обеспечения, τ_{22} - среднее время подключения базы с сигнатурами вирусного программного обеспечения в антивирусе, τ_{33} - среднее время сравнение кода зараженного программного обеспечения с вирусной базой данных, τ_{44} - среднее время поиска в зараженном элементе код вредоносного программного обеспечения, τ_{55} среднее время удаление вредоносного кода., τ - среднее время для всей цепи событий.

Вероятность излечения элемента будет иметь вид (13):

$$P_{из} = f(t)(\square t). \quad (13)$$

Для перехода к плотности вероятности, необходимо взять производную от вероятности, полученной при помощи моделирования сети Петри – Маркова (14).

$$f(t) = P'(t) = \left(1 - e^{-\frac{t}{\tau_0+\tau}}\right) = \frac{e^{-\frac{t}{\tau_0+\tau}}}{\tau_0+\tau}. \quad (14)$$

где, Δt - время дискретизации, причем $\Delta t < f_{max}$; τ_0 - среднее время прохождения сети Петри-Маркова заражения элемента; τ - среднее время прохождения сети Петри-Маркова излечения элемента.

Для нахождения Δt предположим, что функция является убывающей. Значит, максимальное значение она принимает в точке 0. Отсюда следует, что (15):

$$\Delta t = \frac{1}{nf_{\max}} = \frac{1}{n\frac{1}{\tau_0+\tau}} = \frac{\tau_0+\tau}{n}. \quad (15)$$

Вероятность излечения элемента будет иметь вид (16):

$$p_{из} = \frac{e^{-\frac{t}{\tau_0+\tau}}}{\tau_0+\tau}\frac{\tau_0+\tau}{n}. \quad (16)$$

Для нахождения вероятности латентного инфицирования элемента необходимо смоделировать процесс заражения с помощью сети Петри-Маркова. Для построения сети были использованы следующие термины:

S_1—злоумышленник готов к отправки вредоносного программного обеспечения,

S_2—устройство пользователя готово к приему вредоносного программного обеспечения,

t_1—определение способа отправки вредоносного программного обеспечения,

S_3—выбранный способ отправки вредоносного программного обеспечения,

t_2—настройка вредоносного программного обеспечения под выбранный тип отправки определяемы на шаге t_1,

S_4—вредоносное программного обеспечения готово к отправке,

S_5—выбранный способ отправки,

t_3—отправка вредоносного программного обеспечения на устройств,

S_6—вредоносное программного обеспечения находится на устройстве,

Граф данной сети представлен на рис. 3.

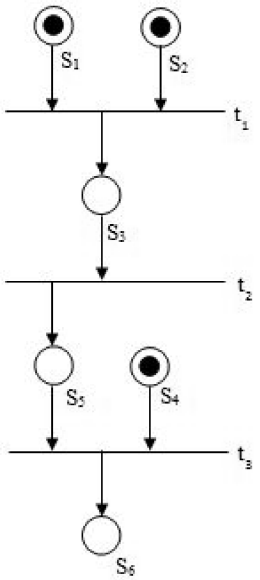

Рис. 3 Граф сети Петри-Маркова реализации латентного заражения программного обеспечения

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений (17):

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_{S_2t_1}(t) = \pi_{21}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_1(t) = \int_0^t f_{S_1t_1}(\tau)\,\Phi_{S_2t_1}(t) + f_{S_1t_1}(\tau)\Phi_{S_1t_1}(t), \quad (17)$$
$$\Phi_{S_3t_2}(t) = \pi_{32}\int_0^t f_{S_3t_2}(\tau)\Phi_1(t-\tau)d\tau,$$
$$\Phi_{S_4t_3}(t) = \pi_{43}\int_0^t f_{S_4t_3}(\tau)d\tau,$$
$$\Phi_{S_5t_3}(t) = \pi_{53}\int_0^t f_{S_5t_3}(\tau)\Phi_1(t-\tau)d\tau,$$
$$\Phi_2(t) = \int_0^t f_{S_4t_3}(\tau)\,\Phi_{S_5t_3}(t) + f_{S_5t_3}(\tau)\Phi_{S_4t_3}(t).$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид (18):

$$f_{S_it_j} = \alpha_{ij}e^{-\alpha_{ij}t}, \quad (18)$$

Где $\alpha_{ij} = 1/\tau_{ij} i = 1,\ldots,6; j = 1,\ldots,3.$

Используя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода (19).

$$\tau_1 = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11}+\tau_{21}},$$
$$\tau_2 = \tau_1 + \tau_{32}, \quad (19)$$
$$\tau_3 = \tau_2 + \tau_{53},$$
$$\tau = \frac{(\tau_2^2+\tau_{53})^2 + (\tau_2+\tau_{53})\tau_{43} + \tau_{43}^2}{(\tau_2+\tau_{53}) + \tau_{43}},$$

где, исходные параметры атаки принимают следующие значения:

τ_{11} - среднее время подготовки вредоносного программного обеспечения злоумышленником, τ_{21} - среднее время подготовки устройства пользователя, τ_{32} = - среднее время настройки вредоносного программного обеспечения под выбранный тип отправки, τ_{43} - среднее время подготовки вредоносного программного обеспечения, τ_{53} - среднее время отправки вредоносного программного обеспечения на устройств, τ - среднее время для всей цепи событий.

Вероятность латентного инфицирования элемента будет иметь вид (20):

$$P_{ли} = f(t)(\square t). \quad (20)$$

Для перехода к плотности вероятности, необходимо взять производную от вероятности, полученной при помощи моделирования сети Петри – Маркова (21).

$$f(t) = P'(t) = \left(1 - e^{-\frac{t}{\tau_0 - \tau}}\right) = \frac{e^{-\frac{t}{\tau_0 - \tau}}}{\tau_0 - \tau}. \quad (21)$$

где, Δt - время дискретизации, причем $\Delta t < f_{max}$; n – шаг дискретизации; τ_0 - среднее время прохождения сети Петри-Маркова заражения элемента; τ - среднее время прохождения сети Петри-Маркова латентного заражения.

Для нахождения Δt предположим, что функция является убывающей. Значит, максимальное значение она принимает в точке 0. Отсюда следует, что (22):

$$\Delta t = \frac{1}{n f_{\max}} = \frac{1}{n\frac{1}{\tau_0 - \tau}} = \frac{\tau_0 - \tau}{n}. \quad (22)$$

Вероятность латентного инфицирования элемента будет иметь вид (23):

$$p_{ли} = \frac{e^{-\frac{t}{\tau_0 - \tau}}}{\tau_0 - \tau}\frac{\tau_0 - \tau}{n}. \quad (23)$$

Для нахождения вероятности выхода из строя инфицирования элемента необходимо смоделировать данный процесс с помощью сети Петри-Маркова. Для построения сети были использованы следующие термины:

S_1—зараженный элемент компьютерной системы,

t_1—анализ элемента с целью изменения его структуры кода,

S_2—элемент не защищен от записи и следовательно есть возможность изменения его функционала,

t_2—замена функционала зараженного элемента вирусным программным обеспечением,

S_3—измененный элемент системы,

t_3—запуск измененного элемента,

S_4—элемент больше не имеет прежнего функционала, следовательно вышел из строя.

Граф данной сети представлен на рис. 4.

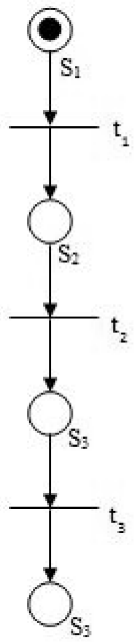

Рис. 4 Граф сети Петри-Маркова реализации выхода из строя зараженного элемента компьютерной системы
компьютерной системы.

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений (24):

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$
$$\Phi_{S_2t_2}(t) = \pi_{22}\int_0^t f_{S_2t_2}(\tau)\Phi_{S_1t_1}(t - -\tau)d\tau, \quad (24)$$
$$\Phi_{S_3t_3}(t) = \pi_{33}\int_0^t f_{S_3t_3}(\tau)\Phi_{S_2t_2}(t-\tau)d\tau,$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид (25):

$$f_{S_it_j} = \alpha_{ij}e^{-\alpha_{ij}t}, \quad (25)$$

Где $\alpha_{ij} = 1/\tau_{ij} i = 1,\ldots,3; j = 1,\ldots,3.$

Используя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода (26).

$$\tau = \tau_{11} + \tau_{22} + \tau_{33}, \quad (26)$$

где, исходные параметры атаки принимают следующие значения:

τ_{11} - среднее время необходимое анализа элемента с целью изменения его структуры кода, τ_{22} - среднее время необходимое для замены функционала зараженного элемента вирусным программным обеспечением, τ_{33} -

среднее время запуска измененного элемента.

Вероятность выхода из строя элемента будет иметь вид (27):

$$P_{вс} = f(t)(\square t). \quad (27)$$

Для перехода к плотности вероятности, необходимо взять производную от вероятности, полученной при помощи моделирования сети Петри – Маркова (28):

$$f(t) = P'(t) = \left(1 - e^{-\frac{t}{\tau_0+\tau}}\right) = \frac{e^{-\frac{t}{\tau_0+\tau}}}{\tau_0+\tau}. \quad (28)$$

где, Δt - время дискретизации, причем $\Delta t < f_{max}$; n – шаг дискретизации; τ_0 - среднее время прохождения сети Петри-Маркова заражения элемента;

τ - среднее время прохождения сети Петри-Маркова выхода из строя.

Для нахождения Δt предположим, что функция является убывающей. Значит, максимальное значение она принимает в точке 0. Отсюда следует, что (29):

$$\Delta t = \frac{1}{nf_{\max}} = \frac{1}{n\frac{1}{\tau_0+\tau}} = \frac{\tau_0+\tau}{n}. \quad (29)$$

Вероятность выхода из строя инфицированного элемента будет иметь вид (30):

$$p_{вс} = \frac{e^{-\frac{t}{\tau_0+\tau}}}{\tau_0+\tau}\frac{\tau_0+\tau}{n}. \quad (30)$$

Литература

1. Брайант Э.Р Компьютерные системы: Архитектура их программирования / Рэндал Э.Брайант, Дэвид Р.О'Халларон.: БВХ-Петербург, 2005. – 1090 с.
2. Радько Н.М., Скобелев И.О. Риск-модели информационно телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М: РадиоСофт. 2010. -232с.
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин.: ДМК Пресс , 2013 – 592 с.
4. Борисов В.И., Радько Н.М., Вероятностные аналитические модели сетевой атаки с внедрением вредоносного программного обеспечения / Информация и безопасность 2013. Т. 16. №1, С485-530.
5. Радько Н.М., Голозубов А.В., Макаров О.Ю. Задача риск-анализа атак «вредоносами» / Информация и безопасность.: Т.15.№1.С.139-140.

Воронежский государственный технический университет
Voronezh state technical university

PROBABILITY SIMULATION RESEARCH ON THE IMPACT FILE VIRUSES ELEMENT COMPUTER SYSTEM

N.M. Radko, D.N. Bocharov

This article describes a model based on Petri nets-Markov process to describe infection element computer system. The probabilities: latent infection cell infection control element, the failure of the infected cell, healing element

Key words: network, the probability file