УДК 004.056

МОДЕЛЬ ОЦЕНКИ ТРУДОЕМКОСТИ УСТРАНЕНИЯ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ В КОРПОРАТИВНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Груздева Л.М.

Российский университет транспорта (МИИТ), Москва, e-mail: docentglm@gmail.com

Распространение вредоносных программ, с помощью которых злоумышленники реализуют угрозы на информационные ресурсы компьютерных сетей, следует рассматривать как вредоносное воздействие. С помощью вредоносного программного обеспечения злоумышленники получают персональные данные пользователей и коммерческую тайну организаций, учетные данные от различных сервисов и систем, что позволяет совершать кибератаки на внутреннюю инфраструктуру сети. Причиной успешных атак на информационные ресурсы следует считать неэффективную организацию защитных механизмов корпоративных сетей передачи данных, не обеспечивающую требуемый уровень противодействия вредоносным воздействиям. В статье предложена математическая модель, на основе использования которой возможно определение наиболее важных характеристик процесса устранения вредоносных воздействий, в том числе математического ожидания времени устранения воздействий, математического ожидания времени поиска заданного числа вредоносных воздействий, дисперсии этих величин и т.д., в условиях ограниченного времени (ресурсов), а также при последовательном устранении вредоносных воздействий в режиме неограниченного времени. Использование предложенной математической модели позволит не только оценить трудоемкость устроения вредоносных воздействий в узлах сети, но оценить качество функционирования корпоративной сети в различные моменты времени в зависимости от начального числа вредоносных воздействий.

Ключевые слова: корпоративная сеть передачи данных, система защиты информации, вредоносное программное обеспечение, вредоносное воздействие

MODEL OF ELIMINATION OF HARMFUL INFLUENCES IN CORPORATE NETWORKS OF DATA TRANSMISSION

Gruzdeva L.M.

Russian University of transport (MIIT), Moscow, e-mail: docentglm@gmail.com

The spread of malware, through which cybercriminals implement threats to the information resources of computer networks, should be considered as a harmful effect. With the help of malicious software, attackers receive personal data of users and commercial secrets of organizations, credentials from various services and systems, which allows them to commit cyber attacks to the internal network infrastructure. The reason for successful attacks on information resources should be considered inefficient organization of corporate network protection mechanisms, which does not provide the required level of counteraction to harmful effects. The article proposes a mathematical model based on the use of which it is possible to determine the most important characteristics of the process of eliminating harmful effects, including the mathematical expectation of the time for elimination of impacts, the mathematical expectation of the time for searching for a given number of harmful effects, the dispersion of these quantities, etc. in conditions of limited time (resources), as well as with the consequent elimination of harmful effects in the regime of unlimited time. Using the proposed mathematical model will allow not only to estimate the complexity of the arrangement of harmful effects in the nodes of the network, but to assess the quality of the corporate network at various times, depending on the initial number of harmful effects.

Keywords: corporate networks of data transmission, information security system, malicious software, harmful effects

Эффективная эксплуатация систем защиты информации (СЗИ) корпоративных сетей передачи данных (КСПД), их проектирование и модернизация невозможны без оценки характеристик процесса по обнаружению вредоносных воздействий, процесса восстановления зараженных узлов сети и планирования работ по профилактике заражения. Проблема защиты цифровой информации от вредоносных программ (ВП), таких как компьютерные вирусы, шпионские и троянские программы, сетевые черви, программы-шантажисты и др., является актуальной и значимой в настоящее время [1, 2] несмотря на то, что первый известный вирус был написан в далеком 1981 г., а современный рынок информационных технологий предлагает множество решений по антивирусной защите. Но ни одна система защиты информации не способна блокировать проникновение вредоносного программного обеспечения (ПО) в корпоративную сеть на 100%. Современная СЗИ, включающая систему обнаружения и предотвращения атак и вторжений IPS/IDS, не может гарантировать обнаружения 70% информационных атак, что периодически приводит к значительному возрастанию вредоносного трафика (ВТ) [3, 4].

По данным компании Positive Technologies [5] самым распространенным методом атак стало использование вредоносного программного обеспечения: в I квартале 2018 г. вредоносное ПО применялось в 63% уникальных кибератак (+27% по сравнению с аналогичным пери-

одом 2017 г. [6]). Большую популярность получила троянская программа WannaMine, заразившая по всему миру более 500 000 устройств.

Цель исследования: разработать математическую модель процесса устранения вредоносных воздействий, использование которой обеспечит возможность оценки качества работы СЗИ и функционирования КСПД в различные моменты времени в зависимости от начального числа вредоносных воздействий (вредоносных программ), используемых методов обнаружения и противодействия.

Под вредоносным воздействием будем понимать распространение вредоносных программ в КСПД, любые их действия, которые могут привести к нарушению работоспособности как отдельных узлов, так и сети в целом.

Математическая модель. Для моделирования процесса устранения вредоносных воздействий в узлах КСПД возьмем за основу математическую модель процесса отладки программного обеспечения, предложенную в книге [7] исследователями А.Г. Мамиконовым, В.В. Кульба, А.Б. Шелковым и получившую дальнейшее развитие в диссертации А.И. Крапчатова [8].

Пусть КСПД состоит из множества узлов (компьютерных систем, КС – S), в каждом из которых протекает марковский процесс [9, 10] по устранению вредоносных воздействий. Система S может находиться в одном из дискретных состояний: s_0, s_1,..., s_N, где N – количество вредоносных воздействий (как частный случай, N может быть равно числу вредоносных программ в узле сети), а s_0 – поглощающее состояние, означающее, что все вредоносные воздействия устранены и процесс сканирования узла окончен.

Под устранением вредоносного воздействия (или вредоносной программы) в узле сети будем понимать его обнаружение и моментальное восстановление КС. Интенсивность устранения вредоносных воздействий будем считать пропорциональным их количеству.

Определим результативность сканирования системы S величиной p_{ij} – вероятностью того, что после сканирования в КС, содержащей i $(i = \overline{0, N})$ вредоносных воздействий, останутся необнаруженными j ($j \geq i$ или $j < i$), $(j = \overline{0, N})$, где N – количество вредоносных воздействий до начала сканирования. Зададим распределение p_{ij} в виде матрицы:

$$P = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & \dots & 0 \\ \underbrace{\begin{pmatrix} p_{N,0} \\ p_{N-1,0} \\ \dots \\ p_{i,0} \\ \dots \\ p_{1,0} \end{pmatrix}}_{R} & \underbrace{\begin{pmatrix} p_{N,N} & p_{N,N-1} & \cdots & p_{N,j} & \cdots & p_{N,1} \\ p_{N-1,N} & p_{N-1,N-1} & \cdots & p_{N-1,j} & \cdots & p_{N-1,1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ p_{i,N} & p_{i,N-1} & \cdots & p_{i,j} & \cdots & p_{i,1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ p_{1,N} & p_{1,N-1} & \cdots & p_{1,j} & \cdots & p_{1,1} \end{pmatrix}}_{Q} \end{pmatrix}. \quad (1)$$

Модель базируется на предположении, что после устранения вредоносного воздействия (вредоносной программы) в узле сети появиться вновь оно уже не может, то есть КС приобретает к нему иммунитет. Система может иметь несколько поглощающих состояний, означающих, что процесс сканирования может быть остановлен, но не все вредоносные воздействия устранены.

Методы и средства исследований. Анализ предложенной модели позволил сделать вывод, что наиболее важными характеристиками процесса устранения вредоносных воздействий в условиях ограниченности времени (ресурсов) являются [7, 8]:

1) математическое ожидание (МО) времени устранения j вредоносных воздействий ($j \geq i$ или $j < i$), $(i, j = \overline{0, N})$:

$$N(n) = 1 + Q + Q^2 + \dots + Q^n,$$

где n – количество циклов обнаружения вредоносных воздействий;

2) МО времени устранения всех вредоносных воздействий в компьютерной системе:

$$t(n) = N(n)\varepsilon,$$

где ε – единичный вектор-столбец;

3) вероятность устранения всех вредоносных воздействий в компьютерной системе:

$$B(n) = R + QR + \dots + Q^{n-1}R;$$

4) МО времени, в течение которого в компьютерной системе существует постоянное число вредоносных воздействий:

$$M_i[r_i(n)] = \frac{1 - p_{ii}^{n+1}}{1 - p_{ii}};$$

5) вероятность того, что в компьютерной системе находится j вредоносных воздействий:

$$h_{ij}(n) = 1 - \prod_{\mu=1}^{n}\left(1 - p_{ij}^{\mu}\right),$$

где $h_{ij}(n)$ – элементы матрицы $H(n)$.

При последовательном устранении вредоносных воздействий (или вредоносных программ) в узлах компьютерной сети в режиме неограниченного времени можно определить следующие наиболее важные характеристики трудоемкости процесса [7, 8]:

1) МО времени устранения всех вредоносных воздействий в компьютерной системе:

$$t = \begin{pmatrix} \sum_{i=1}^{N} \frac{1}{p_{i,i-1}} \\ \sum_{i=1}^{N-1} \frac{1}{p_{i,i-1}} \\ \ldots \\ \sum_{i=1}^{1} \frac{1}{p_{i,i-1}} \end{pmatrix},$$

где $p_{i,i-1}$ – вероятность того, что после одного сканирования в КС будет i – 1 вредоносных воздействий;

2) дисперсия времени устранения всех вредоносных воздействий в компьютерной системе:

$$t_D = \begin{pmatrix} \left(\frac{2}{p_{N,N-1}} - 1\right)\left(\sum_{i=1}^{N}\frac{1}{p_{i,i-1}}\right) + \ldots + \left(\frac{2\cdot 1}{p_{1,0}p_{1,0}} - 1\right) - \left(\sum_{i=1}^{N}\frac{1}{p_{i,i-1}}\right)^2 \\ \left(\frac{2}{p_{N-1,N-2}} - 1\right)\left(\sum_{i=1}^{N-1}\frac{1}{p_{i,i-1}}\right) + \ldots + \left(\frac{2\cdot 1}{p_{1,0}p_{1,0}} - 1\right) - \left(\sum_{i=1}^{N-1}\frac{1}{p_{i,i-1}}\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \left(\frac{2\cdot 1}{p_{1,0}} - 1\right)\left(\frac{1}{p_{1,0}}\right) - \left(\frac{1}{p_{1,0}}\right)^2 \end{pmatrix};$$

3) вероятность устранения всех вредоносных воздействий в компьютерной системе:

$$B = \begin{pmatrix} 1 \\ 1 \\ \ldots \\ 1 \end{pmatrix},$$

то вероятность устранения всех вредоносных воздействий стремится к единице;

4) МО времени, в течение которого в компьютерной системе существует постоянное число вредоносных воздействий:

$$\{M_i[r_i]\} = \begin{pmatrix} \frac{1}{p_{N,N-1}} \\ \frac{1}{p_{N-1,N-2}} \\ \ldots \\ \frac{1}{p_{1,0}} \end{pmatrix};$$

5) дисперсия времени, в течение которого в компьютерной системе существует постоянное число вредоносных воздействий:

$$\{D_i[r_i]\} = \begin{pmatrix} \frac{1 - p_{N,N-1}}{p_{N,N-1}} \\ \frac{1 - p_{N-1,N-2}}{p_{N-1,N-2}} \\ \ldots \\ \frac{1 - p_{1,0}}{p_{1,0}} \end{pmatrix};$$

6) вероятность того, что в КС находится j вредоносных воздействий:

$$H = \begin{pmatrix} 1 - p_{N,N-1} & 1 & \ldots & 1 \\ 0 & 1 - p_{N-1,N-2} & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 - p_{1,0} \end{pmatrix}.$$

На основе представленной математической модели процесса устранения вредоносных воздействий в узлах компьютерной сети можно получить характеристики процесса распространения вредоносных программ.

Рассмотрим компьютерную сеть передачи данных как сеть массового обслуживания [11, 12], в которой циркулируют пакеты в соответствии с маршрутной матрицей $P = \|p_{ij}\|$, где p_{ij} – вероятность пересылки пакета из i-го в j-й узел, причем $\forall\ p_{ij} \geq 0\ \ (i, j = \overline{1, M})$ и $\sum_{j=0}^{M} p_{ij} = 1\ \ \forall i = \overline{1, M}$.

Пусть в качестве пакета в КСПД попадает вредоносная программа, тогда в сети будет протекать случайный процесс распространения ВП. Сеть может находиться в одном из дискретных состояний: $s_1, s_2, ..., s_M$, где $s_i\ \ (i = \overline{1, M})$ означает, что ВП находится в i-м узле.

Важными с практической точки зрения являются следующие вопросы:

1. Сколько шагов будет совершено до остановки процесса распространения ВП, то есть поглощения в том или ином состоянии?
2. Каково время распространения вредоносной программы в сети?
3. Какой узел будет заражен раньше остальных?

Продемонстрируем ответы на поставленные вопросы на примере сети, состоящей из пяти узлов, пакеты в которой пересылаются в соответствии с матрицей:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ p_{21} & p_{22} & p_{23} & p_{24} & p_{25} \\ 0 & 0 & 1 & 0 & 0 \\ p_{41} & p_{42} & p_{43} & p_{44} & p_{45} \\ p_{51} & p_{52} & p_{53} & p_{54} & p_{55} \end{pmatrix}. \qquad (2)$$

С помощью преобразований приведем матрицу (1) к блочной форме:

$$P = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline p_{31} & p_{32} & p_{33} & p_{34} & p_{35} \\ p_{41} & p_{42} & p_{43} & p_{44} & p_{45} \\ p_{51} & p_{52} & p_{53} & p_{54} & p_{55} \end{array}\right). \qquad (3)$$

На основании (3) получена матрица, называемая фундаментальной:

$$M = (I - Q)^{-1}, \qquad (4)$$

где I – единичная матрица;

Q – квадратная подматрица переходов:

$$Q = \begin{pmatrix} p_{33} & p_{34} & p_{35} \\ p_{43} & p_{44} & p_{45} \\ p_{53} & p_{54} & p_{55} \end{pmatrix}.$$

Каждый элемент матрицы (4) соответствует среднему числу раз попадания системы в то или иное состояние до остановки процесса распространения ВП. Умножение справа матрицы M на единичный вектор ε позволяет получить общее среднее количество раз попадания системы в то или иное состояние до поглощения:

$$M' = M \cdot \varepsilon.$$

Зная время пребывания системы в каждом состоянии, можно вычислить общее время до поглощения T':

$$T' = \tau \cdot M',$$

где вектор τ – время пребывания системы в каждом невозвратном состоянии.

Матрица (2) описывает переходы сети, имеющей два поглощающих состояния. Обозначим через b_{ij} вероятность того, что процесс завершится в некотором поглощающем состоянии s_j при условии, что начальным было состояние $s_i\ \ (i, j = \overline{1, M})$. Вероятности b_{ij} образуют матрицу B, строки которой соответствуют невозвратным состояниям, а столбцы – всем поглощающим состояниям:

$$B = M \cdot R, \qquad (5)$$

где $R = \begin{pmatrix} p_{31} & p_{32} \\ p_{41} & p_{42} \\ p_{51} & p_{52} \end{pmatrix}$.

Анализ матрицы (5) позволяет оценить и сравнить вероятности заражения восприимчивых узлов и при построении защиты обезопасить наиболее уязвимые.

Для наглядности произведем вычисления для системы, переходы в которой заданы следующей матрицей:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0,2 & 0,12 & 0,1 & 0,08 & 0,5 \\ 0 & 0 & 1 & 0 & 0 \\ 0,06 & 0,2 & 0,24 & 0,4 & 0,1 \\ 0,27 & 0,2 & 0,1 & 0,23 & 0,2 \end{pmatrix}.$$

По формуле (5) получим матрицу:

$$B = \begin{pmatrix} 0,608 & 0,392 \\ 0,404 & 0,596 \\ 0,606 & 0,394 \end{pmatrix}.$$

Таким образом, если процесс распространения ВП начался из третьего узла сети, то вероятность заражения первого узла равна 0,608, а второго – 0,392.

Для оценки характеристик процесса устранения вредоносных воздействий в КСПД разработана математическая модель, базирующаяся на теории сетей массового обслуживания. На основе предложенной модели возможна не только оценка характеристик процесса устранения вредоносных воздействий, но и процесса распространения ВП в сети. Применение модели наиболее целесообразно для определения вероятности и времени тотального инфицирования корпоративной сети. Предсказание данных характеристик информационных атак, реализуемых с помощью вредоносного программного обеспечения, и трудоемкости по устранению вредоносных воздействий позволит более эффективно использовать средства противодействия и уменьшать последствия данных воздействий.

Список литературы

1. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / под ред. П.П. Парамонова. – СПб: Изд-во ООО «Студия «НП-Принт», 2012. – 115 с.

2. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК, 2014. – 702 с.

3. Груздева Л.М. Повышение производительности корпоративной сети АСУ в условиях воздействия угроз информационной безопасности / Л.М. Груздева, М.Ю. Монахов // Известия высших учебных заведений. Приборостроение. – 2012. – Т. 55, № 8. – С. 53–56.

4. Монахов Ю.М. Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях воздействия вредоносных программ: монография / Ю.М. Монахов, Л.М. Груздева; Владим. гос. ун-т им. А.Г. и Н.Г. Столетовых. – Владимир: Изд-во ВлГУ, 2013. – 132 с.

5. Актуальные киберугрозы I квартал 2018 года [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics (дата обращения: 26.06.18).

6. Актуальные киберугрозы – 2017: тренды и прогнозы [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics (дата обращения: 26.06.18).

7. Мамиконов А.Г. Достоверность, защита и резервирование информации в АСУ / А.Г. Мамиконов, В.В. Кульба, А.Б. Шелков. – М.: Энергоатомиздат, 1986. – 304 с.

8. Крапчатов А.И. Модели и методы планирования разработки и отладки программного обеспечения автоматизированных информационно-управляющих систем: дис. на соиск. учен. степ. канд. техн. наук: (05.25.05) / Александр Иванович Крапчатов; РГГУ. – Москва, 2009. – 136 с.

9. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок. – М.: Книга по Требованию, 2013. – 429 с.

10. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения: учебное пособие / Е.С. Вентцель, Л.А. Овчаров. – 5-е изд., стер. – М.: КноРус, 2016. – 448 с.

11. Маталыцкий М.А. Системы и сети массового обслуживания: анализ и применения: монография / М.А. Маталыцкий, О.М. Тихоненко, Е.В. Колузаева. – Гродно: ГрГУ, 2011. – 816 с.

12. Вишневский В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. – М.: Техносфера, 2003. – 512 с.