05.13.18

Н.А. Семыкина, В.И. Суворов, И.А. Шаповалова

Тверской государственный университет,
математический факультет,
кафедра компьютерной безопасности и математических методов управления,
Тверь, Semykina.NA@tversu.ru, Shapovalova.IA@tversu.ru, Vladimir.Suvorov@mail.ru

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

Для оценки и прогноза динамики процесса подавления деструктивных воздействий кибератак на информационный ресурс создана математическая модель, представленная системой нелинейных дифференциальных уравнений. Построенная модель исследована на устойчивость. Анализ проводился с помощью первого метода Ляпунова. Получены условия существования устойчивого положения равновесия.

Ключевые слова: *математическое моделирование, компьютерная атака, устойчивость системы.*

В настоящее время остро стоит вопрос обеспечения информационной безопасности компьютерных систем. По статистическим данным [1] на сегодняшний день наиболее распространенной причиной (59%) нарушения работы сети государственных учреждений, оборонных предприятий и крупных организаций – это целенаправленные кибератаки (APT-атаки). Атака APT превосходит обычные киберугрозы, так как ориентируется на взлом конкретной цели и готовится на основании информации о ней, собираемой в течение длительного времени. APT осуществляет взлом целевой инфраструктуры посредством эксплуатации программных и аппаратных уязвимостей и методов социальной инженерии [2]. Выделяют 4 стадии целевой атаки (подготовка, проникновение, распространение, достижение цели), каждая из которых сопровождается деятельностью, направленной на сокрытие следов присутствия в системе. Основным способом противостояния целевым атакам является недопущение их начала, поскольку активную атаку крайне сложно заметить. Если атака все-таки была начата, или есть предположение о её наличии, ставится задача обнаружения и локализации. Хотя существует целый комплекс различных мер, направленных на обнаружение APT, они, зачастую, оказываются малоэффективны [3]. Для создания эффективных контрмер требуется всестороннее исследование проблемы. Одним из подходов к анализу распространения вредоносных программ в информационных системах является математическое моделирование, которое позволяет рассмотреть различные сценарии последствий кибератак. Построим математическую модель, описывающую управление мерами защиты в компьютерной системе.

Процесс защиты от кибератак будем рассматривать на временном интервале [0, T]. Предположим, что один и тот же информационный ресурс могут одновременно атаковать несколько хакерских групп. Обозначим через $x_i(t)$ – количество компьютерных атак на инфраструктуру ресурса i-й группировкой в момент времени t. При построении математической модели будем исходить из того, что противоборствующие стороны придерживаются только своей тактики ведения кибератак, не принимая во внимание активность другой противоборствующей стороны. Интенсивность атак злоумышленников зависит от коэффициента интенсивности $\alpha_i(t)$, а также от уровня развития информационных технологий I_i. Информационная система пытается подавить атаки в объеме, равном $z(t)$ с интенсивностью $\beta_i(t)$. Успех защищающейся стороны зависит от ее технологического уровня I и эффективности подавления кибервторжения $\gamma_i(t)$.

В соответствии с вышеперечисленными предположениями имеем следующую систему дифференциальных уравнений с начальными условиями

$$\begin{cases} \dfrac{dx_i}{dt} = \alpha_i(t)x_i(t)\left(1-\dfrac{x_i(t)}{I_i}\right) - \beta_i(t)z(t), \quad x_i(0) = x_{i0}, i = \overline{1,n}; \\ \dfrac{dz}{dt} = \left(\sum\limits_{i=1}^{n}\gamma_i(t)x_i(t)\right)\left(1-\dfrac{z(t)}{I}\right), \quad z(0) = z_0. \end{cases}$$

Исследуем построенную модель на устойчивость. Для анализа задачи рассмотрим сценарий, когда информационную систему атакуют две кибергруппировки, т.е. i = 1, 2. Предположим, что параметры модели являются постоянными: $\alpha_i(t) = \alpha_i$, $\beta_i(t) = \beta_i$, $\gamma_i(t) = \gamma_i$. В этом случае динамическая система имеет следующий вид

$$\begin{cases} \dfrac{dx_1}{dt} = \alpha_1 x_1(t)\left(1-\dfrac{x_1(t)}{I_1}\right) - \beta_1 z(t), \quad x_1(0) = x_{10}, \\ \dfrac{dx_2}{dt} = \alpha_2 x_2(t)\left(1-\dfrac{x_2(t)}{I_2}\right) - \beta_2 z(t), \quad x_2(0) = x_{20}, \\ \dfrac{dz}{dt} = \left(\sum\limits_{i=1}^{2}\gamma_i x_i(t)\right)\left(1-\dfrac{z(t)}{I}\right), \quad z(0) = z_0. \end{cases}$$

Предположим, что существуют положения равновесия. Рассматривая различные варианты равенства нулю множителей третьего уравнения системы, и учитывая, что все параметры и функции модели должны быть неотрицательными значениями, получаем нетривиальные точки равновесия:

$$p_1^* = \left(x_1^*, x_2^*, z^*\right) = \left(\frac{\alpha_1 I_1 + b_1}{2\alpha_1}, \frac{\alpha_2 I_2 + b_2}{2\alpha_2}, I\right),$$

$$p_2^* = \left(x_1^*, x_2^*, z^*\right) = \left(\frac{\alpha_1 I_1 - b_1}{2\alpha_1}, \frac{\alpha_2 I_2 + b_2}{2\alpha_2}, I\right),$$

$$p_3^* = \left(x_1^*, x_2^*, z^*\right) = \left(\frac{\alpha_1 I_1 + b_1}{2\alpha_1}, \frac{\alpha_2 I_2 - b_2}{2\alpha_2}, I\right),$$

$$p_4^* = \left(x_1^*, x_2^*, z^*\right) = \left(\frac{\alpha_1 I_1 - b_1}{2\alpha_1}, \frac{\alpha_2 I_2 - b_2}{2\alpha_2}, I\right),$$

где $b_1 = \sqrt{\alpha_1^2 I_1^2 - 4\alpha_1 I_1 \beta_1 I}$, $b_1 = \sqrt{\alpha_2^2 I_2^2 - 4\alpha_2 I_2 \beta_2 I}$.

Заметим, что в силу физического смысла задачи все значения точек устойчивость положительны, т.е. $x_1^*>0$, $x_2^*>0$, $z^*>0$.

Применим метод Ляпунова по первому приближению в окрестности точек равновесия [3]. Матрица коэффициентов линеаризованной системы будет иметь вид

$$J(p_i^*) = \begin{pmatrix} \alpha_1 - 2\dfrac{\alpha_1}{I_1}x_1^* - \lambda & 0 & -\beta_1 \\ 0 & \alpha_2 - 2\dfrac{\alpha_2}{I_2}x_2^* - \lambda & -\beta_2 \\ \alpha_1\left(1-\dfrac{z^*}{I}\right) & \alpha_2\left(1-\dfrac{z^*}{I}\right) & -\dfrac{(\alpha_1 x_1^* + \alpha_2 x_2^*)}{I} - \lambda \end{pmatrix}.$$

Используя значения точек равновесия, получаем характеристическое уравнение третьего порядка

$$\left(\alpha_1 - 2\frac{\alpha_1}{I_1}x_1^* - \lambda\right)\left(\alpha_2 - 2\frac{\alpha_2}{I_2}x_2^* - \lambda\right)\left(-\frac{(\alpha_1 x_1^* + \alpha_2 x_2^*)}{I} - \lambda\right) = 0.$$

Отсюда довольно легко найти решение этого уравнения

$$\lambda_1 = \alpha_1 - 2\frac{\alpha_1}{I_1}x_1^*, \quad \lambda_2 = \alpha_2 - 2\frac{\alpha_2}{I_2}x_2^*, \quad \lambda_3 = -\frac{(\alpha_1 x_1^* + \alpha_2 x_2^*)}{I}.$$

Для устойчивости динамической системы действительная часть всех собственных значений матрицы устойчивости должна быть отрицательна. Для λ_3 это условие выполняется всегда. Исследуем другие собственные числа.

$$\lambda_1 < 0, \text{ если } x_1^* > \frac{I_1}{2}. \quad \lambda_2 < 0, \text{ если } x_2^* > \frac{I_2}{2}.$$

Отсюда следует, что точки равновесия p_2^*, p_3^*, p_4^* не удовлетворяют этим ограничениям, следовательно, в окрестности этих точек динамическая система не является устойчивой, а точка p_1^* является устойчивой.

Данные условия означают, что кибергруппировки для реализации компьютерных атак должны использовать более половины своего технологического резерва, а защищаемая информационная система для успешного отражения атак – весь свой технологический потенциал.

Как было сказано выше, современные APT-атаки имеют сложный сценарий проникновения и захвата информационных ресурсов, поэтому для построения адекватной модели рассмотрим параметры интенсивности атак $\alpha_i(t)$, как функции времени. Возможны различные случаи.

Если компьютерные атаки носят волнообразный характер, т. е. увеличиваются к определенному моменту времени t^*, а затем снижаются до нуля, то для описания параметра интенсивности можно выбрать тригонометрическую функцию.

$$\alpha_i(t) = A_i \sin\left(\frac{\pi}{2t^*}t\right) + k_i, \; A_i,\ k_i - \text{положительные константы.}$$

Случай, когда кибергруппировка сначала реализует подготовительный этап вторжения, а затем в определенный момент времени t^* проводят лавинообразную атаку, можно описать с помощью степенной функции.

$$\alpha_i(t) = A_i\left(t - t^*\right)^n + k_i, \; A_i,\ k_i - \text{положительные константы.}$$

Сценарий, когда достигнув своего максимума в информационных технологиях I_i, с течением времени интенсивность атак не изменяется, можно описать логарифмической функцией.

Если на определенном промежутке времени интенсивность атак падает, то происходящие можно описать через обратную тригонометрическую функцию.

Аналогичные ситуации можно рассмотреть и для параметров, характеризующие действия защищаемой информационной системы.

В ходе проведенной работы разработана модель противодействия компьютерным атакам. Модель может найти применение в обеспечении информационно-аналитической поддержки принятия управленческих решений в сфере компьютерной безопасности.

Список литературы

1. Кибербезопасность 2019—2020: тенденции и прогнозы. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/ (дата обращения: 20.04.2021).
2. *Левцов В., Демидов Н.* Анатомия таргетированной атаки, часть 1// Information Security/ Информационная безопасность. - 2016. - № 2. — С. 36 - 39. (дата обращения: 20.04.2021).
3. *Левцов В., Демидов Н.* Анатомия таргетированной атаки, часть 3// Information Security/ Информационная безопасность. - 2016. - № 4. — С. 40-45. URL: http://lib.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki. (дата обращения: 20.04.2021).
4. *Демидович Б.П.* Лекции по математической теории устойчивости. – СПб.: Лань, 2008.