УДК 519.7

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ РАСПРОСТРАНЕНИЯ СЕТЕВЫХ ЧЕРВЕЙ В ИЗОЛИРОВАННОЙ КОРПАРОТИВНОЙ СЕТИ

Красулин А.Ю., Яковлев М.М., студенты гр. ИБс-231, III курс
Научный руководитель: Кузнецова А.В., к.т.н., доцент
Кузбасский государственный технический
университет имени Т.Ф. Горбачёва
г. Кемерово

Стремительная цифровизации порождает новые векторы угроз в компьютерных сетях, среди которых особое место занимают само распространяющиеся вредоносные программы (сетевые черви). В условиях, когда периметральные средства защиты могут быть преодолены с помощью социальной инженерии, критически важной становится задача прогнозирования скорости распространения угрозы внутри сети [1]. Эмпирические эксперименты на живой инфраструктуре недопустимы из-за риска отказа в обслуживании, поэтому основным методом исследования выступает математическое моделирование.

Целью данной работы является построение и численный анализ детерминированной модели распространения червя в локальной сети для оценки эффективности различных стратегий реагирования.

Математическая постановка задачи

В качестве базового аппарата выбрана компартментальная теория, адаптированная для задач информационной безопасности. Рассматривается замкнутая сеть из N узлов. В каждый момент времени t хосты распределены по трем непересекающимся классам: $S(t)$ (уязвимые, но здоровые), $I(t)$ (инфицированные распространители) и $R(t)$ (изолированные или пропатченные).

Динамика процесса описывается системой нелинейных обыкновенных дифференциальных уравнений (ОДУ) [2]:

$$\begin{cases} \dfrac{dS}{dt} = -\beta \dfrac{S(t)I(t)}{N} \\ \dfrac{dI}{dt} = \beta \dfrac{S(t)I(t)}{N} - \gamma I(t) \\ \dfrac{dR}{dt} = \gamma I(t) \end{cases}$$

Где β – коэффициент интенсивности сканирования и заражения, а γ – показатель эффективности мер реагирования (обратная величина от среднего времени устранения угрозы).

Обоснование метода решения

Ключевой особенностью данной системы является наличие нелинейного члена $S(t)I(t)$, описывающего взаимодействия узлов. Из-за этого система **не имеет точного аналитического решения**, выражаемого через элементарные функции. Найти прямую зависимость $I(t)$ в виде формулы невозможно без существенных упрощений, которые снизили бы точность прогноза.

В связи с этим для решения задачи применяется **численное моделирование.** Мы используем метод конечных разностей (метод Эйлера), который позволяет перейти от дифференциальных уравнений к системе рекуррентных формул. Это дает возможность рассчитать состояние сети в любой момент времени t_{k+1} на основе данных предыдущего шага t_k с шагом дискретизации Δt.

Рекуррентные формулы для программной реализации выглядят следующим образом:

1. *Уязвимые узлы:*

$$S_{k+1} = S_k - \left(\frac{\beta}{N} \cdot S_k \cdot I_k\right) \cdot \Delta t$$

2. *Инфицированные узлы:*

$$I_{k+1} = I_k + \left(\frac{\beta}{N} \cdot S_k \cdot I_k - \gamma \cdot I_k\right) \cdot \Delta t$$

3. *Защищенные узлы:*

$$R_{k+1} = R_k + (\gamma \cdot I_k) \cdot \Delta t$$

Численный эксперимент

Для апробации модели выбрана типовая сеть отдела, состоящая из 200 рабочих станций ($N = 200$). В начальный момент времени ($t = 0$) происходит инцидент: один узел заражается ($I_0 = 1$), остальные уязвимы ($S_0 = 199$). Шаг моделирования $\Delta t = 0{,}1$ часа.

Расчет производится итерационным методом Эйлера. Состояние системы на шаге $k + 1$ определяется по значениям шага k с учетом приращений за время $\Delta t = 0{,}1$ часа.

Сценарий №1: Отсутствие активного противодействия

Входные параметры: $\beta = 0{,}8$ (агрессивный червь), $\gamma = 0{,}05$ (медленная реакция).

Начальные условия: $(t = 0)$: $S_0 = 199, I_0 = 1, R_0 = 0$.

Шаг 1 $(t = 0{,}1)$:

Вычисляем скорости изменения состояний:

$$\frac{dS}{dt} = -0{,}8 \cdot \frac{199 \cdot 1}{200} = -0{,}796$$

$$\frac{dR}{dt} = 0{,}05 \cdot 1 = 0{,}05$$

$$\frac{dI}{dt} = -\frac{dS}{dt} - \frac{dR}{dt} = 0{,}796 - 0{,}05 = 0{,}746$$

Получаем новые значения:

$$S_1 = 199 + (-0{,}796 \cdot 0{,}1) = 198{,}92$$

$$I_1 = 1 + (0{,}746 \cdot 0{,}1) = 1{,}075$$

$$R_1 = 0 + (0{,}05 \cdot 0{,}1) = 0{,}005$$

Проверка баланса: $198{,}92 + 1{,}075 + 0{,}005 = 200$.

Шаг 2 ($t = 0{,}2$):

Используем значения S_1, I_1, R_1:

$$\frac{dS}{dt} = -0{,}8 \cdot \frac{198{,}92 \cdot 1{,}075}{200} \approx -0{,}855$$

$$\frac{dR}{dt} = 0{,}05 \cdot 1{,}075 \approx 0{,}054$$

$$\frac{dI}{dt} = 0{,}855 - 0{,}054 = 0{,}801$$

Получаем новые значения:

$$S_2 = 198{,}92 + (-0{,}855 \cdot 0{,}1) = 198.83$$

$$I_2 = 1{,}075 + (0{,}801 \cdot 0{,}1) = 1{,}155$$

$$R_2 = 0{,}005 + (0{,}054 \cdot 0{,}1) = 0{,}01$$

Наблюдается уверенный рост числа инфицированных (I), так как скорость заражения значительно превышает скорость лечения.

Как показало моделирование (рис. 1), при таких параметрах наблюдается взрывной рост. Пик эпидемии достигается на 10-м часу, когда зараженными оказываются одновременно 146 компьютеров (73% сети).

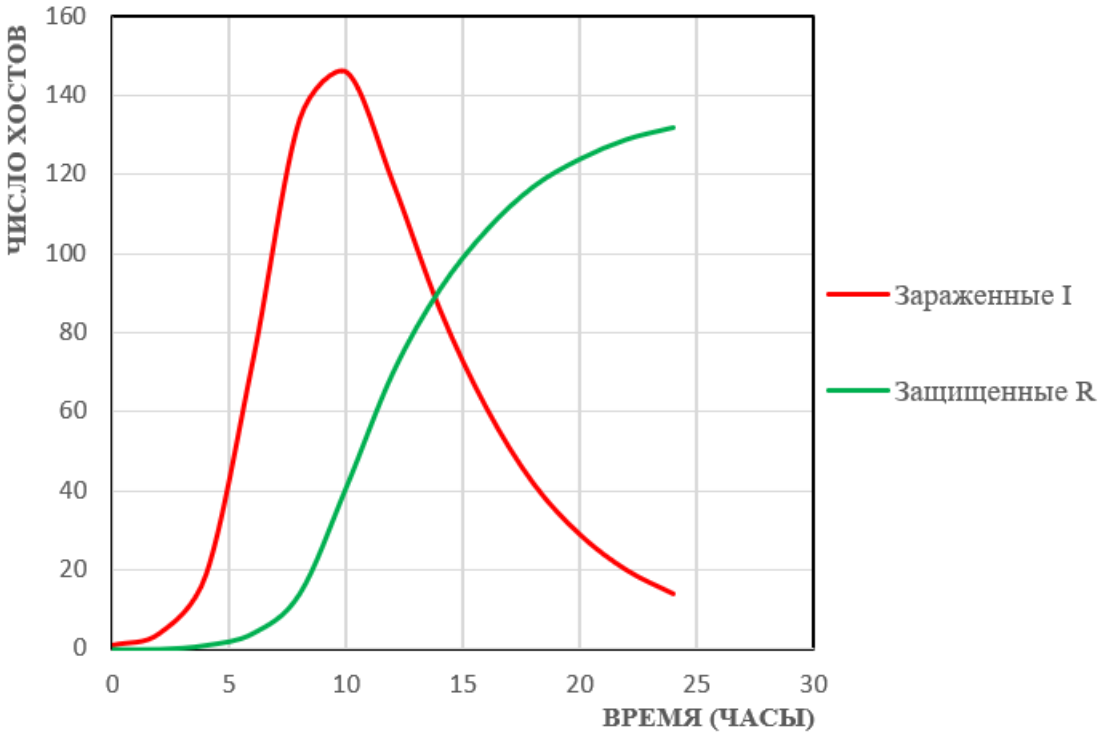

Рисунок 1 – Динамика заражения при низкой скорости реакции

Сценарий №2: Оперативная блокировка

Входные параметры: $\beta = 0{,}8$ (агрессивный червь), $\gamma = 0{,}4$ (медленная реакция).

Начальные условия: $(t = 0)$: $S_0 = 199, I_0 = 1, R_0 = 0$.

Шаг 1 ($t = 0{,}1$):

$$\frac{dS}{dt} = -0{,}8 \cdot \frac{199 \cdot 1}{200} = -0{,}796$$

$$\frac{dR}{dt} = 0{,}4 \cdot 1 = 0{,}4$$

$$\frac{dI}{dt} = -\frac{dS}{dt} - \frac{dR}{dt} = 0{,}796 - 0{,}4 = 0{,}396$$

Получаем новые значения:

$$S_1 = 199 + (-0{,}796 \cdot 0{,}1) = 198{,}92$$

$$I_1 = 1 + (0{,}396 \cdot 0{,}1) = 1{,}04$$

$$R_1 = 0 + (0{,}4 \cdot 0{,}1) = 0{,}04$$

Шаг 2 ($t = 0{,}2$):

Используем значения S_1, I_1, R_1:

$$\frac{dS}{dt} = -0{,}8 \cdot \frac{198{,}92 \cdot 1{,}04}{200} \approx -0{,}827$$

$$\frac{dR}{dt} = 0{,}4 \cdot 1{,}04 \approx 0{,}416$$

$$\frac{dI}{dt} = 0{,}827 - 0{,}416 = 0{,}411$$

Получаем новые значения:

$$S_2 = 198{,}92 + (-0{,}827 \cdot 0{,}1) = 198.84$$

$$I_2 = 1{,}04 + (0{,}411 \cdot 0{,}1) = 1{,}08$$

$$R_2 = 0{,}04 + (0{,}416 \cdot 0{,}1) = 0{,}08$$

При увеличении скорости реакции в 8 раз характер кривой меняется (рис. 2). Количество одновременно зараженных узлов не превышает 38 единиц. Существенная часть сети (более 40 хостов) успевает перейти в защищенное состояние R, минуя стадию заражения.

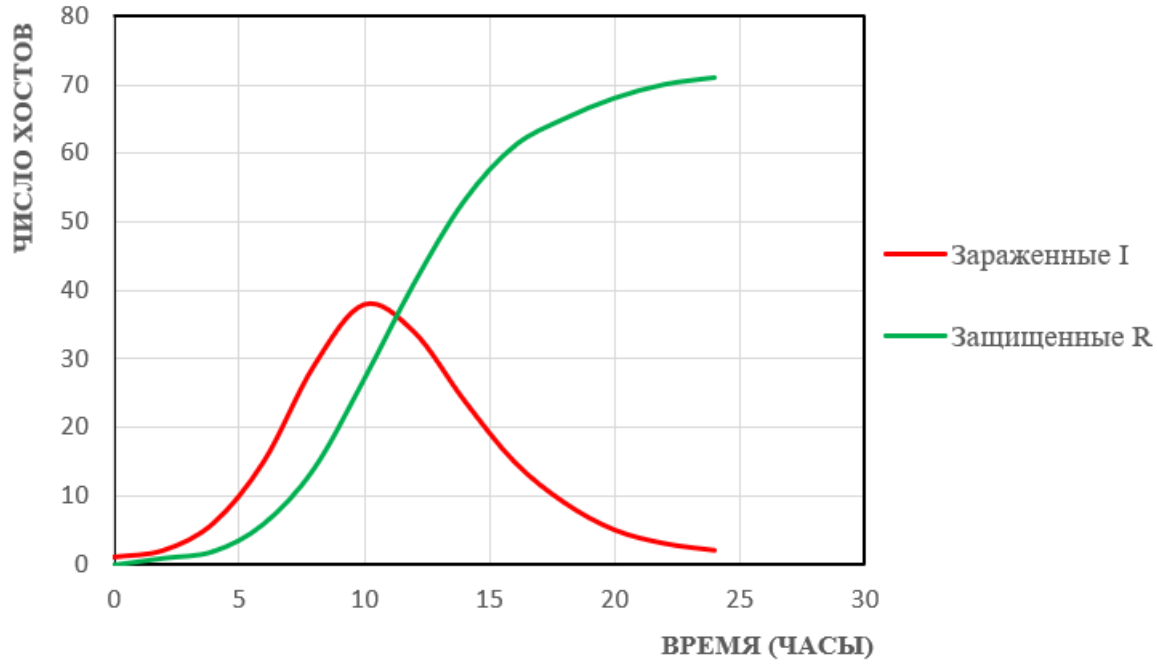

Рисунок 2 – Сглаживание пика атаки при оперативных мерах

Сравнительный анализ:

К моменту времени $t = 0{,}2$ в первом сценарии число зараженных выросло до $1{,}155$, а во втором – только до $1{,}08$. При этом количество защищенных узлов во втором сценарии $(0{,}08)$ уже в 8 раз выше, чем в первом $(0{,}01)$. Это математически подтверждает эффективность повышения параметра γ.

Заключение

Разработанная численная модель на базе рекуррентных соотношений доказала необходимость внедрения автоматизированных средств защиты. Расчеты показали, что даже при высокой агрессивности червя ($\beta = 0{,}8$) своевременное повышение параметра γ (скорости реакции) позволяет снизить пиковую нагрузку в 3,8 раза и предотвратить полный паралич сети. Полеченные алгоритмы могут быть интегрированы в другие системы для прогнозирования ущерба в реальном времени.

Список литературы:

1. Макаренко, С. И. Информационная безопасность: учебное пособие для студентов вузов / С. И. Макаренко. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. URL: https://fileskachat.com/view/32175_fc6906f15e47134cd597b8857eab7556.html

2. Кузнецов, О. П. Дискретная математика для инженера / О. П. Кузнецов. – 6-е изд., стер. – СПб.: Лань, 2009. – 400 с. URL: https://djvu.online/file/SBqZ3D54yHJMN