РАЗДЕЛ VI. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 001.891.573, 004.056.53

МОДЕЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБРАБОТКЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МАТЕМАТИЧЕСКОГО АППАРАТА ДИСКРЕТНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

О.О. Евсютин, В.Г.Миронова

В настоящей статье рассматриваются вопросы построения моделей на основе математического аппарата дискретных динамических систем. Представлена модель несанкционированного доступа в информационную систему на основе сети Петри-Маркова. Введено два типа обобщенных моделей преобразования информации на основе клеточных автоматов и в качестве расширения одной из обобщенных моделей рассмотрена модель сжатия цифровых изображений на основе клеточных автоматов.

Ключевые слова: сети Петри-Маркова, клеточные автоматы, информационная безопасность, обработка данных.

Модель несанкционированного доступа на основе цепи Маркова

Случайный процесс, протекающий в информационной системе, называется Марковским или случайным процессом без последствия, если для любого момента времени t_0 вероятность любого состояния системы при $t > t_0$ зависит только от ее состояния при $t = t_0$ и не зависит от того, как и когда система пришла в это состояние. Если число состояний, которые может принимать система, конечно, то такие системы описывает Марковский случайный процесс с дискретным состоянием, или Марковская цепь [1].

Модель несанкционированного доступа в информационную систему описывает процесс реализации атаки (последовательность атакующих действий), при котором для любого момента времени t_0 вероятность любого состояния атаки при $t > t_0$ зависит только от ее состояния при $t = t_0$ и не зависит от того, как и когда атака достигла этого состояния. В связи с этим модель несанкционированного доступа в информационную систему можно считать Марковским процессом. Поскольку атака направлена на осуществление несанкционированного доступа в информационную систему, то конечным состоянием атаки будет получение несанкционированного доступа в информационную систему, поэтому данную модель можно рассматривать как Марковскую цепь.

Потоком событий называется некоторая последовательность однотипных событий, которые происходят в случайные моменты времени и относятся к случайным процессам с дискретным состоянием и непрерывным временем. Если события в потоке происходят поодиночке, а не группами из нескольких событий, то такой поток называется ординарным. Ординарный поток без последствия называется потоком Пуассона. Важнейшей характеристикой любого потока событий является его интенсивность — среднее число событий, произошедших в потоке за одну единицу времени λ [2].

Модель несанкционированного доступа в информационную систему описывает атаку со стороны нарушителя, то есть последовательность действий, которые необходимо совершить злоумышленнику. Последовательность действий нарушителя при осуществлении атаки будет представлять собой поток событий. Поскольку действия нарушителя при проведении атаки (потоке событий) будут совершаться поодиночке, то этот поток будет являться ординарным потоком. Характеристикой любого потока событий является его интенсивность $\lambda(t)$ — среднее число событий, произошедших в потоке за одну единицу времени. Для реализации атаки нарушителей информационной безопасности, представленной в виде Марковского случай-

ного процесса с дискретным состоянием и непрерывным временем, интенсивность потока событий не зависит от времени, поэтому $\lambda(t) = \lambda = \text{const}$, и этот поток событий будет являться стационарным потоком Пуассона. Стационарный поток Пуассона называется простейшим потоком.

Для простейшего потока Пуассона, средний интервал времени между двумя событиями $\tau_{ср} = \frac{N}{\lambda}$, где N — количество переходов между событиями. А поскольку рассматривается интервал времени одного перехода между двумя событиями, то $N = 1$.

Для простейшего потока вероятность появления потока m событий за время t равна

$$P_m = \frac{(\lambda \cdot t)^m \cdot e^{-\lambda \cdot t}}{m!},$$

где

P_m — вероятность появления потока m событий;

λ — интенсивность потока;

t — время осуществления потока событий;

m — количество совершенных событий.

Вероятность непоявления ($m = 0$) события за время τ равна

$$P_0 = \frac{(\lambda \cdot \tau)^0 \cdot e^{-\lambda \cdot t}}{0!} = e^{-\lambda \cdot t}.$$

Вероятность появления хотя бы одного события P_1 вычисляется следующим образом:

$$P_1 + P_0 = 1;$$

$$P_1 = 1 - P_0 = e^{-\lambda \cdot t}.$$

С целью управления вероятностью успешной реализации несанкционированных действий по времени (с использованием статических данных) построим аналитические модели несанкционированного доступа в информационную систему на основе сетей Петри-Маркова.

Построение аналитических моделей для основных видов несанкционированного доступа в информационную систему предлагается осуществлять в следующей последовательности:

1. Сценарий атаки делится на множества событий $S = \{s_1, s_2, ..., s_n\}$, $s_n \in S$ и условий $T = \{t_1, t_2, ..., t_n\}$, $t_n \in T$;
2. На основе введенных множеств событий и условий строится граф сети Петри-Маркова;
3. Записываются основные элементы матрицы, определяющие логические функции срабатывания сети;
4. Сеть Петри-Маркова описывается системой интегро-дифференциальных уравнений;
5. Находится среднее время перемещения по сети Петри-Маркова из начальной позиции до конечного перехода на основе пуассоновского приближения;
6. Определяется вероятность успеха проведения атаки [3–5].

На рисунке 1 представлена модель воздействия угроз безопасности конфиденциальной информации (УБКИ) на защищаемый объект.

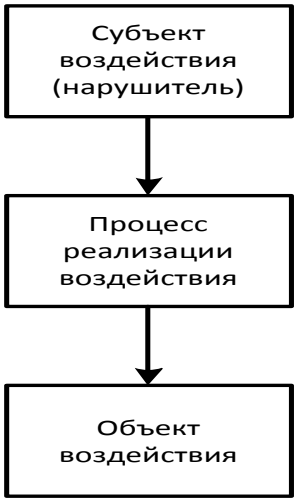

Рисунок 1— Модель воздействия УБКИ на защищаемый объект

Модели преобразования данных на основе клеточных автоматов

Другим примером дискретных динамических систем, использующихся для моделирования в информационной безопасности и обработке данных, являются клеточные автоматы [6].

Можно описать два типа моделей, построенных с использованием математического аппарата теории клеточных автоматов, и описывающих разного рода процессы преобразования (кодирования) информации.

В первом случае преобразование входных данных осуществляется непосредственно клеточным автоматом, как это показано на рисунке 2.

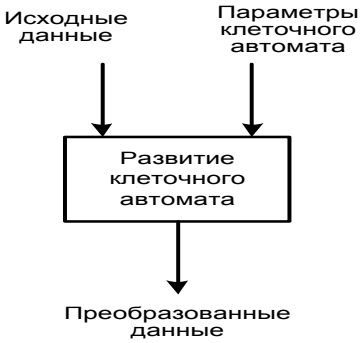

Рисунок 2 — Модель преобразования данных в процессе развития клеточного автомата

В рамках представленной модели наиболее значимыми являются следующие свойства клеточного автомата:

1. Изменение энтропии в процессе развития клеточного автомата;
2. Скорость распространения информации по решетке клеточного автомата;
3. Изменение корреляции между соседними состояниями решетки (между начальным и конечным состоянием решетки) для заданного клеточного автомата.

В соответствии с данной моделью строятся, в частности, криптографические алгоритмы симметричного шифрования и хэширования [7]. Здесь же следует отметить, что модель, представленная на рисунке 2, является обобщенной, и конкретные приложения клеточных автоматов опираются на ее расширения, что выражается в появлении дополнительных входов. Например, в случае шифрования появляется дополнительный параметр — секретный ключ.

Во втором случае преобразование заключается в сопоставлении элементам данных некоторых кодов, вырабатываемых клеточным автоматом. Соответствующая модель представлена на рисунке 3.

В рамках данной модели основными являются следующие свойства клеточного автомата:

1. Влияние начального состояния решетки с определенным образом упорядоченной структурой на историю развития клеточного автомата;
2. Способность порождать в ходе развития клеточного автомата последовательности (коды) заданного вида.

Данная модель, как и рассмотренная ранее, также является обобщенной, и конкретные приложения теории клеточных автоматов опираются на ее расширения. Одним из таких расширений является модель сжатия цифровых изображений на основе клеточных автоматов, описанная в [8].

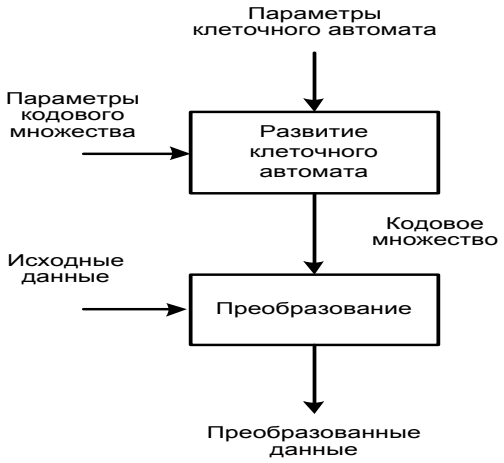

Рисунок 3 — Модель преобразования данных с использованием кодового множества, получаемого с помощью динамики клеточного автомата

Остановимся на некоторых особенностях данной модели.

Ее основу составляет декоррелирующее клеточное преобразование, представляющее собой преобразование элементов цифрового изображения к виду, когда между ними отсутствует пространственная избыточность, построенное с использованием динамики клеточного автомата.

Декоррелирующее клеточное преобразование осуществляется по формуле (1)

$$G = C \cdot F \cdot C^T, \qquad (1)$$

где

C— базис преобразования, представляющий собой квадратную $n \times n$ матрицу, строки которой обладают свойством попарной взаимной ортогональности, $C = \left(c_{ij}\right)_{i=1,j=1}^{n,n}$, $c_{ij} \in R$;

F— блок элементов цифрового изображения, матрица той же размерности, что и C, $F = \left(f_{ij}\right)_{i=1,j=1}^{n,n}$, $f_{ij} \in Z$.

Векторы базиса C представляют собой состояния из некоторой истории развития k-битового клеточного автомата, под которым будем понимать клеточный автомат с алфавитом внутренних состояний, содержащим число элементов, выражаемое k-ой степенью двойки, то есть $|A| = 2^k$, $k \in Z$. Использование подобных клеточных автоматов удобно в плане практической реализации вычислительного метода.

Нетривиальный базис может быть ортогональным только в том случае, если его элементы принимают как отрицательные, так и положительные значения. Поскольку алфавит внутренних состояний клеточного автомата представляет собой отрезок ряда целых чисел, вводится отображение $\kappa : A \to B$, которое целочисленному значению каждой клетки ставит в соответствие элемент из специальным образом заданного множества базисных коэффициентов B.

Элементы множества B выбираются из отрезка $[-1; 1]$, причем количество положительных и отрицательных значений выбирается примерно равным, чтобы обеспечить чередование знаков в базисных векторах.

При построении множеств базисных коэффициентов для различных клеточных автоматов на разбиении лучше оперировать малыми целочисленными и рациональными величинами. В качестве знаменателя рациональных величин имеет смысл выбирать степени двойки, чтобы операция деления в процессе вычислений могла быть заменена сдвигом на соответствующее количество бит.

Теперь введем классификацию множеств базисных коэффициентов с точки зрения их внутреннего устройства (отметим, что данная классификация вводится исключительно в рамках настоящей работы и не претендует на универсальность).

1. Симметричное множество. Множество B назовем симметричным, если $\forall b \in B$ существует $b' = -b$, $b' \in B$, и B можно определить как $B = \{-b_{2^{k-1}}, ..., -b_1, b_1, ..., b_{2^{k-1}}\}$.
2. Множество, симметричное относительно нуля. Множество B назовем симметричным относительно нуля, если его можно представить в виде $B = B' \cup \{0\}$, где B' — симметричное множество, соответственно, $B = \{-b_{2^{k-1}-1}, ..., -b_1, b_0 = 0, b_1, ..., b_{2^{k-1}-1}\}$ Мощность такого множества не может быть выражена степенью двойки, поэтому при построении базиса декоррелирующего преобразования нуль должен ставиться в соответствие двум различным элементам алфавита внутренних состояний.
3. Асимметричное множество.

Множество B назовем асимметричным, если оно представимо в виде $B \setminus \{0\} = B' \cup B''$, где $b' < 0 \quad \forall b' \in B'$ и $b'' > 0 \quad \forall b'' \in B''$, и $|B'| \neq |B''|$, либо существует хотя бы один элемент $b' \in B'$, что $-b' \notin B''$.

Примеры множеств базисных коэффициентов согласно введенной классификации представлены в таблице 1.

Таблица 1 — Примеры множеств базисных коэффициентов

Тип	Число бит	Множество
Симметричное	1	$\{-1,1\}$
Симметричное относительно нуля	2	$\left\{-\frac{1}{2}, 0, \frac{1}{2}\right\}$
Ассиметричное	3	$\left\{-1, -\frac{3}{4}, -\frac{1}{2}, 0, \frac{1}{4}, \frac{1}{2}, 1\right\}$

Вывод

В заключение следует отметить, что рассмотренная модель сжатия цифровых изображений на основе клеточных автоматов является расширением модели, представленной на рисунке 3, прежде всего по той причине, что динамика клеточного автомата используется не выработки кодового множества, а для построения базиса, который, в свою очередь, и определяет непосредственное преобразование данных [9].

СПИСОК ЛИТЕРАТУРЫ

1. .Котов В.Е. Сети Петри. [Текст] /В.Е. Котов/ — М: Наука, 1984. — 160 с.
2. Шелупанов А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» [Текст] / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // - Доклады ТУСУРа. — 2010. — № 1 (21), ч. 1. — С.14–22.
3. Миронова В. Г. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности [Текст] / В.Г. Миронова, А.А. Шелупанов// - Доклады ТУСУРа. — 2010. — № 2 (22), ч. 1. — С.257–259.
4. Миронова В.Г. Анализ этапов предпроектного обследования информационной системы персональных данных [Текст] / В.Г. Миронова, А.А. Шелупанов // - Вестник СибГАУ им. М.Ф. Решетнева. — 2011. — № 2 (35). — С. 45–48.
5. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях [Текст] / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // - Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

6. Евсютин О.О. Использование клеточных автоматов для решения задач преобразования информации [Текст] / О.О. Евсютин, С.К. Росошек // - Доклады ТУСУРа. — 2010. — № 1(21), часть 1. — С. 173–174.
7. Евсютин О.О. Шифр на основе обратимых клеточных автоматов на разбиении [Текст] / О.О. Евсютин, С.К. Росошек // - Безопасность информационных технологий. — 2007. — № 4. — С. 27–31.
8. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных [Текст] / О.О. Евсютин, А.А. Шелупанов // - Доклады ТУСУРа. — 2012. — № 1(25), часть 2. — С.119–125.
9. Мещеряков Р.В., Крайнов А.Ю., Шелупанов А.А. Модели надежности передачи информации в защищенной распределенной телекоммуникационной сети [Текст] /Р.В. Мещеряков, А.Ю. Крайнов, А.А. Шелупанов// - Известия Томского политехнического университета. Том 313 N5, 2008.- С. 60-63.

***Евсютин О.О.**, аспирант каф. КИБЭВС ФГБОУ ВПО ТУСУР, **Миронова В.Г.**, аспирант каф. КИБЭВС ФГБОУ ВПО ТУСУР*

УДК 004.056.5

СНИЖЕНИЕ ОШИБКИ ОБНАРУЖЕНИЯ DDOS АТАК СТАТИСТИЧЕСКИМИ МЕТОДАМИ ПРИ УЧЕТЕ СЕЗОННОСТИ

О.С. Терновой, А.С. Шатохин

В статье рассматривается задача раннего обнаружения DDOS атак с использованием статистических методов при учете сезонности, в работе сетевого ресурса. Предложена гипотеза раннего диагностирования DDOS атаки. Гипотеза апробирован на данных соответствующих реальным DDOS атакам, полученным из лог файлов различных web серверов. Для апробации алгоритма разработан программный комплекс, в который входят: база данных, программа для экспорта лог файлов в базу данных, программа детектор, которая проводит анализ и диагностирует начало DDOS атаки, различными способами.

Ключевые слова: DDOS атака, распределенная атака, отказ в обслуживании, зомби сеть, BOT сеть, среднеквадратичное отклонение, статистический анализ, ранее обнаружение, Hypertext Preprocessor, сезонность

Введение

DDOS атаки – распределенные атаки направленные на отказ в обслуживании, продолжают оставаться, одной из важнейших угроз в сети. Атаки такого типа могут быстро истощить сетевые ресурсы или мощности сервера, что приведет к невозможности получить доступ к ресурсу, и вызовет серию негативных последствий: упущенная прибыль, невозможность воспользоваться услугами и произвести различные транзакции и т.д[1].

В DDOS атаке в роли атакующего выступает так называемая бот сеть или «зомби» сеть. Зомби сеть может насчитывать от нескольких десятков до тысяч хостов. Обычно это нейтральные компьютеры, которые, в силу каких-то причин (отсутствие файрвола, устаревшие базы антивируса, и т.д.), были заражены, вредоносными программами. Программы, работая в фоновом режиме, непрерывно посылают запросы на атакуемый сервер, выводя его таким образом из строя [2].

В настоящий момент не существует какого-то универсального средства для противодействия DDOS атакам. Даже такие крупные компании как Microsoft, eBay, Amazon, Yahoo страдают от DDOS атак и не всегда могут с ними справиться [2].

Постановка задачи

Для противодействия распределенным атакам, направленным на отказ в обслуживание, требуется выполнение двух основных задач [3].

1. Диагностировать DDOS атаку на самых ранних стадиях. Чем раньше будет обнаружена DDOS атака, тем раньше сможет включиться в игру сетевой администратор и тем раньше можно будет начать проводить анти DDOS мероприятия. Кроме того при обнаружении DDOS атаки, можно будет не дожидаясь реагирования администратора, автоматически запустить мероприятия по противодействию атаки: задействовать резервные каналы связи, включить фильтры, и т.д.
2. Вторая задача связанна с разделением общего потока трафика на вредоносный и обычный. Поняв, какие из клиентских запросов являются результатом DDOS атаки, можно будет создать соответствующие правила для межсетевого экрана или ACL правила для маршрути-