Метод управления кибер устойчивостью на основе математической иммунологии

С. А. Петренко
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
s.petrenko@rambler.ru

К. А. Маковейчук[1], А. В. Олифиров[2]
ФГАОУ ВО «КФУ имени В. И. Вернадского»
[1]christin2003@yandex.ru, [2]alex.olifirov@gmail.com

***Аннотация*. В данной статье рассматривается новый метод управления киберустойчивостью цифровых платформ на основе математической иммунологии. Рассмотрены основные идеи метода. Его существенным достоинством является принципиальная возможность моделирования динамики поведения цифровых платформ в условиях возмущающих воздействий внешней среды. Другим важным достоинством является придание цифровым платформам новых свойств адаптивности и самоорганизации, позволяющих достаточно гибко и адекватно реагировать на возмущения в реальном масштабе времени. Приведен алгоритм обучения иммунной подсистемы управления киберустойчивостью. Рассмотрена аппаратно-программная реализация метода управления киберустойчивостью цифровой платформы на основе математической иммунологии.**

Ключевые слова: метод управления киберустойчивостью; цифровая платформа; математическая иммунология; свойства адаптивности и самоорганизации

I. Введение

«Метод иммунного ответа» – это новый метод противодействия кибератакам. Его существенным достоинством является принципиальная возможность моделирования динамики поведения инфраструктуры предприятия в условиях воздействия различного рода злоумышленников, выявление и парирование ранее не известных атак. Другим важным достоинством является придание системе безопасности свойств адаптивности и самоорганизации, позволяющих достаточно гибко и адекватно реагировать на компьютерные атаки в реальном масштабе времени. Рассмотрим основные идеи метода иммунного ответа, а также его реализацию в соответствующей системе противодействия компьютерным атакам [1, 2, 4, 6–8, 10].

II. Характеристика направления исследований

Разработке метода предшествовали следующие основные исследования в области иммунных систем (рис. 1).

Рис. 1. Классификация методов искусственных иммунных систем

- Хидж и Коуэл построили уравнение, описывающее изменение количества циркулирующих антител в зависимости от числа плазматических клеток.
- Йилек предложил ряд вероятностных моделей взаимодействия антигена с иммунокомпетентной В-клеткой, а также промоделировал методом Монте-Карло процесс образования клона, происходящего из одной В-клетки.
- Белл, используя основные гипотезы клонально-селекционной теории Ф. Бернета, построил математическую модель гуморальной иммунной реакции на неразмножающийся моновалентный антиген. Им же была предложена простейшая модель иммунной реакции на размножающийся антиген, в которой описано взаимодействие между антигеном и антителом.
- Качественное исследование модели «хищник – жертва» было проведено Пимбли, а затем, после введения в модель уравнения для В-клеток, Пимбли, Шу и Казариновым. Аналогичные модельные представления развиваются Смирновой и Романовским.
- В 1974 году итальянские ученые Бруни, Джовенко, Кох и Штрем предложили модель гуморальной иммунной реакции, которая описывает гетерогенность популяции иммуноцитов с помощью непрерывных функций двух аргументов: аффинитета и времени. Основной отличительной чертой модели является рассмотрение иммунной реакции с позиции теории билинейных систем. Дальнейшее развитие эта работа получила в двух направлениях. Молер модифицирует модель с целью описания более широкого круга явлений (производство антител разных классов, кооперация между Т- и В-системами иммунитета и т.д.). С

другой стороны, это работы, которые направлены на решение задачи идентификации исходной модели.

- Академик Г.И. Марчук построил и в дальнейшем уточнил простейшую математическую модель инфекционного заболевания, которая представляет собой систему обыкновенных нелинейных дифференциальных уравнений с запаздывающим аргументом. Кроме реакции «антиген– антитело», эта модель описывает влияние поражения антигеном органа-мишени на динамику иммунного процесса.
- Рихтер и Хоффман предложили оригинальные модели иммунной реакции, в основу которых положена сетевая теория Ерне. Основное внимание в этих моделях уделяется рассмотрению различных событий, протекающих в сети.
- Перельсон рассмотрел иммунную реакцию с позиции теории оптимального управления.
- Мерилл предложил описание иммунной реакции с точки зрения теории катастроф.

Перечислим основные практические наработки в упомянутой области [3, 5, 7–10].

- В Великобритании был реализован проект Computational Immunology for Fraud Detection (CIFD). Цель проекта– разработка системы защиты на базе технологии AIS для почтовой службы Англии (рис. 2).
- В Европе реализован проект разработки сетевой системы обнаружения атак Lisys путем контроля трафика TCP SYN.

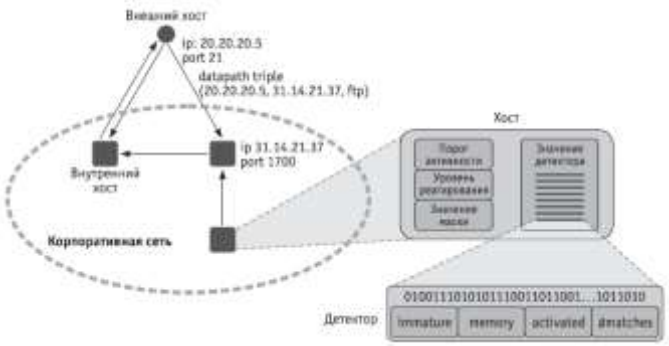

Рис. 2. Возможная архитектура искусственной иммунной системы

- В США разработано расширение к ядру Linux – Process Homeostasis (pH), позволяющее обнаруживать, а при необходимости и замедлять необычное поведение прикладных программ. Для обнаружения необычного поведения первым делом автоматически создаются профили системных вызовов, сделанных различными программами. На создание такого профиля уходит некоторое время, после чего программа может действовать самостоятельно, сначала включая экспоненциальную задержку по времени для аномальных вызовов, а затем и вовсе уничтожая процесс. Так как контролировать все вызовы накладно и нерационально, система работает только с системными вызовами, имеющими полный доступ к ресурсам компьютера (рис. 3).

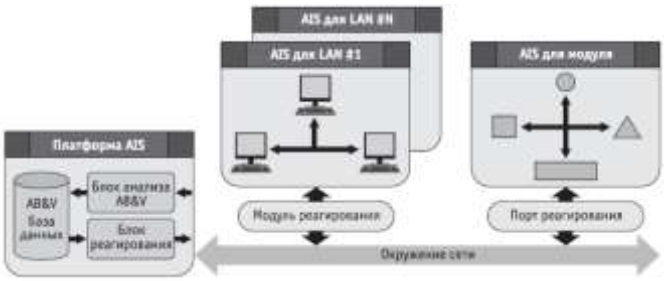

Рис. 3. Структурная схема иммунной системы обнаружения компьютерных атак

- Аналогичный проект STIDE (Sequence Time-Delay Embedding) был призван помочь в обнаружении внедрений, распознавая необычные эпизоды системных вызовов. В процессе обучения STIDE формирует базу данных из всех уникальных, непрерывных системных вызовов и затем делит их на части предопределенной фиксированной длины (рис. 4).

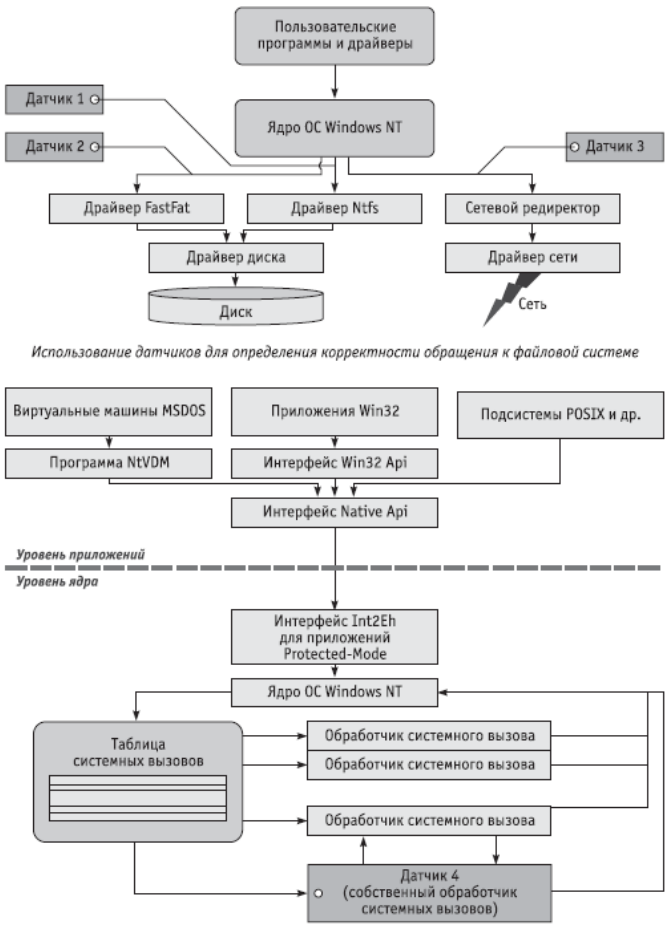

Рис. 4. Элементы технологий иммунного ответа

Во время работы STIDE сравнивает эпизоды, полученные при новых трассировках с уже имеющимися в базе данных, и сообщает о критерии аномалии, указывающем, сколько новых вызовов отличаются от нормы.

III. Математическая постановка задачи

Начальные условия

$$V(t^0) = V^0, C(t^0) = C^0, F(t^0) = F^0 \quad (1)$$

Условия функционирования

Количество аномалий программного обеспечения (ПО) в функционирующей информационной системе (ИС):

$$\frac{dV}{dt} = (\beta - \gamma F)V, \quad (2)$$

где β – коэффициент распространения аномалий по системе, γ – количество обнаруженных аномалий ко времени *dt*.

$$\frac{dC}{dt} = \varepsilon(m)\alpha V(t-\tau)F(t-\tau) - \mu_C(C - C^*), \quad (3)$$

где *ε(m)* – характеристика функционирования ИС при поражении основных программных подсистем, α – коэффициент, характеризующий обнаружение аномалии средством защиты информации (СЗИ), *μc* – коэффициент, характеризующий время жизни вирусов до обновления ПО.

Относительная характеристика поражения системы:

$$\frac{dF}{dt} = \rho C - \left(\mu_f + \eta\gamma V\right)F, \quad (4)$$

$$\frac{dm}{dt} = \sigma V - \mu_m m, \quad (5)$$

где σV – степень поражения ИС, μm – коэффициент пропорциональности, характеризующий величину пери ода восстановления ИС.

Найти

Иммунологический барьер, который характеризует насыщение ИС средствами противодействия компьютерным атакам:

$$V^* = \frac{\mu_f(\gamma + F^* V)}{\beta\eta\gamma} > V^0 > 0. \quad (6)$$

IV. Основные идеи предлагаемого метода

Для решения поставленной задачи была разработана следующая модель воздействия вредоносного ПО на операционную среду ИС (рис. 5).

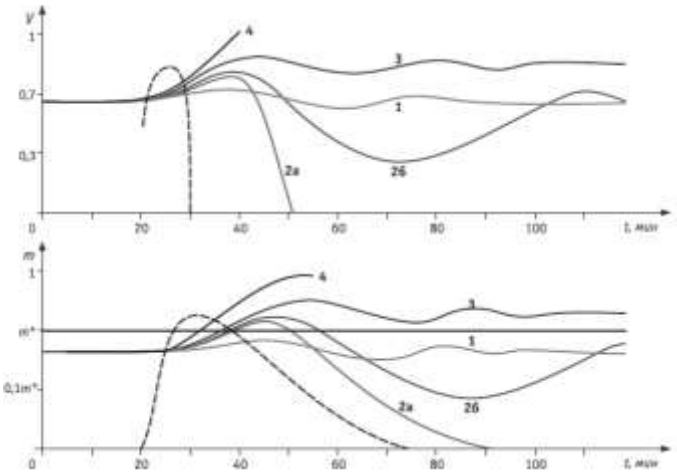

Рис. 5. Качественная картина поражения ИС комбинированным вредоносным ПО

$$\frac{dV_i}{dt} = (\beta_i - \gamma_i F_i)V_i,$$

$$\frac{dF_i}{dt} = q_i C_i - \eta_i\gamma_i F_i V_i - \mu_i F_i,$$

$$\frac{dC_i}{dt} = \xi p_s(V_i)\alpha_i F_i(t-\tau) \times V_i(t-\tau) - \mu_{C_i}(C_i - C_i^*), \quad (7)$$

$$\frac{dm_i}{dt} = \sigma_i V_i - \mu_{m_i} m_i,$$

где $i = \overline{1, N}$ – «номер» разновидности компьютерной атаки;

N – число различных разновидностей компьютерных атак;

$V_i(t)$ – концентрация i-го вредоносного ПО в общем объёме требуемых функций ИС;

$F_i(t)$ – концентрация антител, специфичных к i-му вредоносному программному обеспечению;

$C_i(t)$ – концентрация контрмер обнаружения к i-й компьютерной атаке;

$m_i(t)$ – относительная характеристика поражения ИС i-й атакой, $0 \le m_i \le 1$;

$\xi = \prod_{i=1}^{N} \xi_i(m_i)$ – функция, характеризующая общее состояние ИС;

$\xi_i(m_i)$ – невозрастающая непрерывная функция, характеризующая общее состояние ИС при i-й атаке, $\xi_i(0) = 1, \xi_i(1) = 0, 0 \le \xi_i(m_i) \le 1$.

К системе уравнений (7) присоединим начальные данные при $t = t^0$.

$$V(t^0) = V^0, C(t^0) = C^0. \quad (8)$$

1. Концентрация размножающихся антигенов вредоносного ПО *V(t)*.

2. Концентрация антител *F(t)* (антитела – субстраты иммунной системы операционной среды ИС, нейтрализующие антигены).

3. Концентрация мер наблюдения и предупреждения воздействия вредоносного ПО *C(t).*

4. Относительная характеристика поражения системной среды ИС на *m(t).*

В результате удалось получить следующие основные утверждения.

Утверждение 1. При неотрицательных начальных данных при $t = t^0 = 0$

$$V^0 \geq 0, C^0 \geq 0, F^0 \geq 0, m^0 \geq 0. \quad (9)$$

Решение задачи (1), (2) существует и единственно при всех $t \geq 0$.

Утверждение 2. При всех $t \geq 0$ решение задачи (1), (2) будет непрерывным и неотрицательным:

$$V(t) \geq 0, C(t) \geq 0, F(t) \geq 0, m(t) \geq 0. \quad (10)$$

Утверждение 3. Теорема существования и единственности решения задачи (1), (2) позволяет получить формальные модели поражения ИС вредоносным ПО.

Утверждение 4. Воздействия вредоносного ПО, которые не приводят к потере устойчивости функционирования ИС, удовлетворяют неравенству

$$0 < V_0 < \frac{\mu_f(\gamma F^* - b)}{\beta \eta \gamma} = V^*. \quad (11)$$

Утверждение 5. Величина V^* – иммунологический барьер операционной среды ИС. Иммунологический барьер пройден, если воздействия программного обеспечения V^0 удовлетворяют условию $V^0 > V^*$, и не пройден в противном случае (рис. 6).

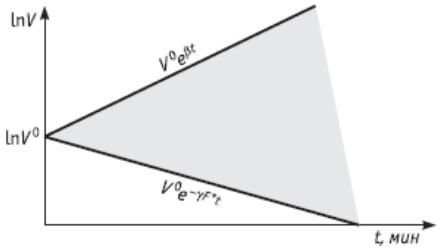

Рис. 6. Область допустимых решений

V. Основные алгоритмы метода иммунного ответа

На рис. 7 отображены задачи, решение которых предполагает практическая реализация метода.

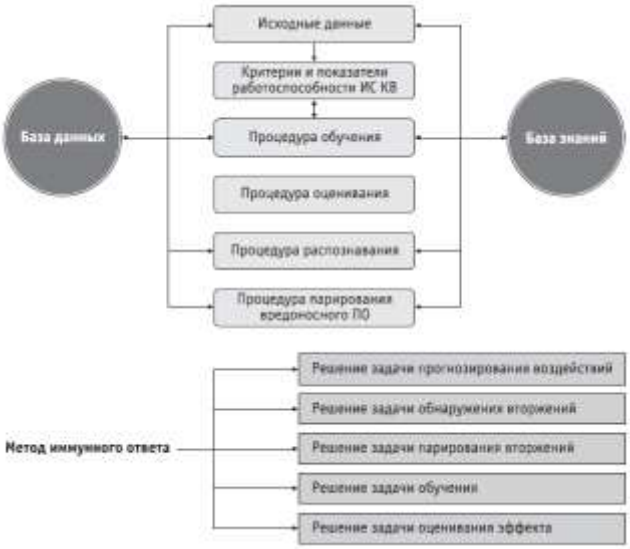

Рис. 7. Основные задачи метода иммунного ответа

Предложенные алгоритмы управления киберустойчивостью были доведены до практической реализации.

Список литературы

[1] Ashby W.R. (1991) Principles of the Self-Organizing System. In: Facets of Systems Science. International Federation for Systems Research International Series on Systems Science and Engineering, vol 7. Springer, MA. DOI: https://doi.org/10.1007/978-1-4899-0718-9_38

[2] Biryukov D.N Cognitive-functional memory specification for simulation of purposeful behavior of cyber systems // Proceedings of SPIIRAS, 2015, Issue. 3 (40), pp. 55-76. DOI: http://dx.doi.org/10.15622/sp.40.5

[3] Biryukov D.N, Lomako A.G. Denotational Semantics of Knowledge Contexts in Ontological Modeling of the Subject Areas of Conflict // Proceedings of SPIIRAS. 2015. Issue. 5 (42). P. 155-179. DOI: http://dx.doi.org/10.15622/sp.42.8

[4] Bongard M.M., Problema uznavaniya [The Problem of Recognition], Moscow: Nauka Publ., 1967.

[5] Kotenko I., Polubelova O., Saenko I., Doynikova E. The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems. [Proc. 2013 International Conference on Availability, Reliability and Security]. Germany, 2013, pp. 638-645. DOI: 10.1109/ARES.2013.84

[6] Kotenko I.V. Intelligent mechanisms of cybersecurity management // In Risk and security management. Proceedings of the Institute of System Analysis of the Russian Academy of Sciences, 2009, Vol.41, pp.74-103.

[7] Mussel L.V. Problems of creating a Smart Grid in Russia from the standpoint of information technology and cyber security [Proc. All-Russian Seminar "Methodological issues of reliability research of large energy systems"]. Irkutsk, ESI SB RAS, 2014, pp. 171-181.

[8] Petrenko S.A., Makoveichuk K.A. Ontology of cyber security of self-recovering smart Grid In CEUR Workshop Proceedings, 2017, Vol-2081, pp. 98–106. http://ceur-ws.org/Vol-2081/paper21.pdf

[9] Petrenko S.A., Petrenko A.S., Makoveichuk K.A. Problem of developing an early-warning cybersecurity system . In CEUR Workshop Proceedings, 2017, Vol-2081, pp. 112–117. http://ceur-ws.org/Vol-2081/paper23.pdf

[10] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty. [Proc. 20th IEEE International Conference on Soft Computing and Measurements]. St. Petersburg, 2017, pp 299-300. DOI: 10.1109/SCM.2017.7970566.