14. Gorelik V.Yu., Bezus M.Yu. On the security of the critical information infrastructure of the Russian Federation. *StudNet*, 2020, no. 9, pp. 1438–1448. (In Russ.)
15. Ljashko D.A., Anikin I.V. Modeling the agent and manager of the remote administration system by means of protecting information from unauthorized access. *Izvestija YuFU. Tehnicheskie nauki*, 2012, no. 12 (137), pp. 96–104. (In Russ.)

Received 11.10.2021

УДК 004.89

АДАПТАЦИЯ МЕХАНИЗМОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ КООПЕРАТИВНОГО ПРОТИВОСТОЯНИЯ УГРОЗАМ ВТОРЖЕНИЯ В АВТОНОМНЫЕ ИНФОТЕЛЕКОММУНИКАЦИОННЫЕ ОБЪЕКТЫ

Скатков А.В., Моисеев Д.В., Брюховецкий А.А.
Севастопольский государственный университет, Севастополь, РФ
E-mail: dmitriymoiseev@mail.ru

В настоящей работе продолжены исследования авторов, посвященные адаптации механизмов искусственных иммунных систем путем модификации классических математических моделей в соответствии со спецификой искусственных иммунных систем, что позволило значительно повысить их эффективность при выполнении прогнозирования состояния объекта контроля – решении задачи идентификации, которая заключается в нахождении мощностей источников деградации ресурсов (вирусной атаки) автономной инфотелекоммуникационной системы по имеющимся экспериментальным данным. В работе предложены модели кооперативного взаимодействия нескольких автономных инфотелекоммуникационных систем, защита которых построена на базе искусственных иммунных систем. Как известно, в настоящее время множество методов, основанных на принципах иммунологии, расширяется, а искусственные иммунные системы вызывают наибольший интерес среди исследователей благодаря свойствам особых механизмов памяти, поиска, распознавания, адаптации и др. В работе впервые предлагается использование механизмов передачи антивирусных баз между искусственной иммунной системой донора и искусственной иммунной системой акцептора. Получены результаты вычислительного эксперимента, свидетельствующие о потенциальной эффективности предлагаемых алгоритмов.

Ключевые слова: *искусственный интеллект, беспилотное средство контроля, искусственные иммунные системы, кооперативные системы*

Введение

Бурное развитие в настоящее время теории и систем искусственного интеллекта (ИИ) и построенных с его использованием автономных беспилотных транспортных средств (БТС) требует уделять большое внимание вопросам защиты информации (ЗИ), накапливаемой, хранимой и обрабатываемой в информационных системах (ИС), которыми и являются БТС [1; 2]. Особую роль в ЗИ БТС занимают вопросы создания систем превентивной ЗИ [3].

Как известно, применение различных эвристических алгоритмов, вдохновленных живой природой, – методов муравьиных колоний, роевого интеллекта, искусственных нейронных сетей, имитации отжига, эволюционные алгоритмы и т. д., используется в первую очередь для решения задач оптимизации [4; 5].

Одним из актуальных классов биоинспирированных алгоритмов в современных исследованиях являются иммунные системы. Методы иммунных систем, ориентированные на решение задачи глобальной оптимизации, основаны на некоторых аспектах поведения иммунной системы человека в процессе защиты ею организма. Защитные клетки иммунной системы (антитела) претерпевают при этом множество изменений, целью которых является создание клеток, обеспечивающих наилучшую защиту. Искусственные иммунные системы (ИИС) обладает основными свойствами искусственного интеллекта: памятью, способностью к обучению и принятию решений в незнакомой ситуации [6; 7].

В работах по биологии и медицине иммунные системы представляют собой сложнейшие децентрализованные системы, способные решать задачу обеспечения жизнедеятельности организма в условиях агрессивной, все время меняющейся окружающей среды [8–11].

В настоящей работе продолжены исследования авторов, начатые в [12] и посвященные адаптации механизмов искусственных иммунных

систем путем модификации классических математических моделей в соответствии со спецификой ИИС, что позволило значительно повысить их эффективность при выполнении прогнозирования состояния объекта контроля – решении задачи идентификации, которая заключается в нахождении мощностей источников вторжений в инфотелекоммуникационные системы по имеющимся экспериментальным данным. Развитие искусственного интеллекта и построенных с его использованием беспилотных транспортных средств позволяет использовать механизмы искусственных иммунных систем для контроля параметров автономных информационных систем.

Постановка задачи

Целью данной работы является адаптация механизмов искусственных иммунных систем для кооперативного противостояния угрозам вторжения в автономные инфотелекоммуникационные системы.

Как показано в работах [12–14], используемые до настоящего времени выражения, описывающие идеализированное поведение поражаемого ресурса (процессора, памяти, канала связи), в которых не учитывается невозможность при определенном уровне поражения ресурса выполнять защитный (иммунный) ответ, модифицированы авторами путем введения невозрастающей неотрицательной функции, учитывающей нарушение нормальной работы ИИС вследствие значительного поражения ресурса. Накапливание антивирусной базы с опережением приносит положительный эффект в скорости уменьшения поражений от вирусных атак и повышении эффективности антивирусных алгоритмов. Также впервые для корректного описания механизмов ИИС для БТС авторами предлагается рассматривать поражения ресурсов БТС вирусами как мультипликативную функцию.

Адаптация механизмов ИИС за счет модификации классических математических моделей в соответствии со спецификой ИИС значительно повышает их эффективность при выполнении прогнозирования состояния интерфейсов БТС – решении задачи идентификации, которая заключается в нахождении мощностей источников атак по имеющимся экспериментальным данным. Развитие ИИ и построенных с его использованием беспилотных средств контроля и мониторинга позволяет использовать механизмы искусственных иммунных систем для контроля интерфейсов автономных инфотелекоммуникационных систем при вторжении.

В соответствии с изложенными фактами и представлениями о динамике иммунного ответа выделим следующие переменные модели, которые являются непрерывными функциями [12]: $V = V(t)$ – мощность деструктивного воздействия вирусов; $C = C(t)$ – относительный размер антивирусной базы; $F = F(t)$ – вычислительная сложность антивирусных алгоритмов; $m = m(t)$ – доля пораженного вирусов ресурса.

Математическая модель адаптированной иммунной реакции на вторжение, в соответствии с [12–14], строится на основе соотношений баланса для каждой из зависимых переменных в предположении, что «организм» описывается однородным замкнутым объемом, в котором все компоненты процесса равномерно перемешаны:

$$\frac{dV}{dt} = \beta V(t) - \gamma F(t) V(t), \quad (1)$$

$$\frac{dF}{dt} = \rho C(t) - \eta\gamma F(t) V(t) - \mu_f F(t),$$

$$\frac{dC}{dt} = \xi(m)\alpha F(t+\tau) V(t-\tau) - \mu_C (C - C''),$$

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

с начальными условиями:

$$V(0) = V^0,\ F(0) = F^0,$$

$$C(0) = C^0,\ m(0) = m^0,$$

и фазовыми ограничениями:

$$V(t) \geq 0.0,\ F(t) \geq 0.0,$$

$$C(t) \geq 0.0,\ m(t) \geq 0.0,$$

где $\beta > 0$ – скорость размножения вирусов; $\gamma > 0$ – коэффициент, учитывающий вероятность определения вируса антивирусом; $\alpha > 0$ – коэффициент стимуляции иммунной системы; $\rho > 0$ – скорость антивирусного алгоритма; $\mu_C > 0$ – величина, обратная продолжительности жизни специфического алгоритма; $\mu_f > 0$ – величина, обратная продолжительности антивирусного алгоритма; $\eta > 0$ – количество операций, необходимое для нейтрализации одного вируса; $\sigma > 0$ – скорость (темп) поражения ресурса; $\mu_m > 0$ – скорость восстановления ресурса; $C'' > 0$ – предсуществующий размер антивирусной базы; $\tau > 0$ – время, необходимое для формирования каскада специфических антивирусных алгоритмов.

В рассматриваемом иммунном ответе участвуют вирусы $V(t)$, антивирусные алгоритмы $F(t)$, антивирусная база $C(t)$ и атакуемый (повреждаемый) ресурс $m(t)$.

Модифицированные математические модели иммунного ответа ИИС с учетом совместного противостояния вторжению

Следует отметить, что предложенная авторами [12; 14] модификация математической модели циклического иммунного ответа ИИС на внешнее вторжение с учетом накопления антивирусной базы с опережением $C^*(t)$ приносит положительный эффект в скорости уменьшения объемов накопленных вирусов $V^*(t)$ и повышении эффективности антивирусных алгоритмов $F^*(t)$, соответственно, появляется потенциальная возможность в случае кооперативной работы нескольких ИИС передать ресурсы одной ИИС, которая в настоящий момент не испытывает враждебных атак, другой ИИС, которая в настоящий момент противостоит атаке.

Рассмотрим три возможных сценария кооперативного взаимодействия двух ИИС с учетом вышеописанного сценария.

1. ИИС, не подверженная атаке, передает второй ИИС в распоряжение свою, превентивно наращенную $C_1^*(t)$. В таком случае выражение (1) для второй ИИС примет вид

$$\frac{dV_2}{dt} = \beta V_2(t) - \gamma F_2(t) V_2(t), \qquad (2)$$

$$\frac{dF_2}{dt} = \rho C_2(t) - \eta\gamma F_2(t) V_2(t) - \mu_f F_2(t),$$

$$\frac{dC_2}{dt} = \xi(m)\alpha F_2(t+\tau) V_2(t-\tau) - \mu_C\left(C_2 - C_2''\right) + C_1,$$

$$\frac{dm_2}{dt} = \sigma V_2(t) - \mu_m m_2.$$

Системы (1) и (2) содержат функции $F(t+\tau)$ и $V(t+\tau)$ аргументов вида $(t\pm\tau)$ и их производные. Такие системы не удовлетворяют, в частности, условиям теоремы Коши о существовании и единственности решений. Их решение (особенно в случае нелинейности в аналитическом виде) неизвестно, однако уравнения подобного типа чрезвычайно актуальны. Они возникают в иммунологии, химии, металлургии редкоземельных элементов, экологических моделях, а также в задачах моделирования вирусных эпидемий и др.

На такие уравнения обратили внимание А.Д. Мышкис [16], Я.З. Ципкин [17], Г.А. Каменский [18], который дал их классификацию и предпринял попытку построить общую теорию уравнений с отклоняющимся аргументом. Тем не менее и сегодня единственным конструктивным методом их решений остаются численные методы типа процедур Адамса, Милна, Рунге – Кута и подобных. Но и здесь, как правило, возникают существенные сложности, обусловленные необходимостью дополнения начальных условий для старших производных, учета потенциально возможных точек разрыва производных, эффектом неустойчивости решений.

Перспективным, на наш взгляд, для системы (2) является:

– использование обобщенных разложений функции V в ряд Тейлора вида:

$$V(t) = \sum_{j=0}^{n} \frac{V'(a)}{j!}(t-a)^i + \sum_{k:x_j<x} \sum_{j=1}^{n} \frac{\delta_k^j}{j!}(t-t_k)^i + R_n(t),$$

где $a < t_1 < t_2 < \cdots < t_m < b$, а величины разрывов производных:

$$\delta_k^j = V^{(i)}(t_k + 0) - V^{(j)}(t_k - 0),$$

$R_n(t)$ – остаточный член;

– разложение функций $V(t)$ по степеням запаздывания τ:

$$V'(t) = \Phi\left[t, V(t), V(t) - \tau V'(t) + \cdots + \frac{(-1)^{m_\tau m}}{m!} V^{(m)}(t)\right].$$

Далее, если обосновывать возможность использования метода малого параметра при старшей производной, то решение можно искать в разложениях по степеням малого запаздывания τ с характеристическим показателем:

$$\lambda(\tau) = 1 - \lambda + \frac{3}{2}\lambda^2 + \frac{8}{3}\lambda^3 + \cdots,$$

что невозможно при переменном запаздывании. Таким образом, при известных оговорках, численное интегрирование системы (2) является по существу безальтернативным подходом к использованию идей ИИС в данном классе задач.

Зависимости, приведенные на рисунке 1, характеризуют иммунный ответ ИИС на воздействие атаки в соответствии с выражением (1) при начальных условиях: относительная концентрация загрязнения (вируса) – 1,0, относительное количество антивирусных клеток – 0,5, относительный объем антиген-специфических клеток – 0,0, поражаемый орган полностью здоров – 0,0.

Как видно из графиков (см. рисунок 1), относительное количество вируса V начинает значительно уменьшаться из-за работы антивирусных алгоритмов F, вычислительная мощность которых, в свою очередь, сначала увеличивается до

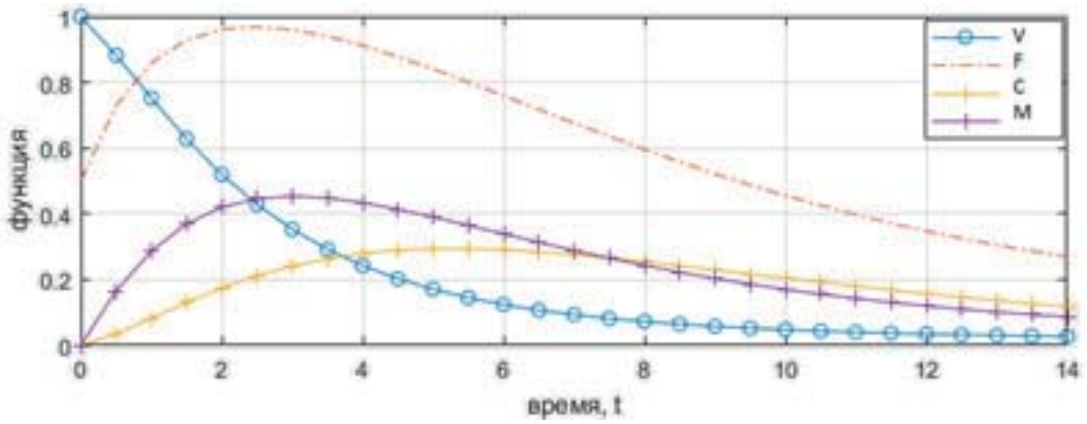

Рисунок 1. Результаты моделирования иммунного ответа ИИС без использования сторонних антивирусных баз

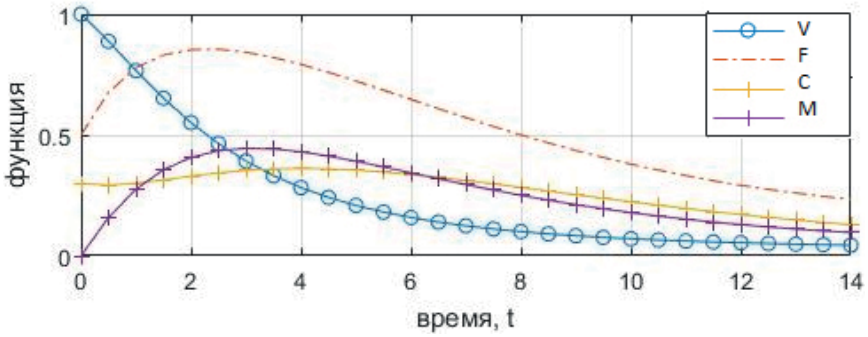

Рисунок 2. Результаты моделирования иммунного ответа ИИС с использованием сторонних антивирусных баз

$t = 2,2,$ затем начинает уменьшаться за счет антивирусной базы C, размер которой сначала увеличивается до достижения максимума $(t = 5,0)$, после чего постоянно уменьшается. После победы антивируса над вирусом скорость уменьшения расходования антивирусной базы C замедляется. Поражаемый ресурс, в свою очередь, испытывает на себе поражающее воздействие вирусов и угнетающее воздействие от производства избыточного объема антивирусной базы, максимум поражения ресурса приходится на $t = 5,0,$ после чего он начинает постепенно восстанавливаться. После превышения в относительном объеме антивирусных алгоритмов над вирусами $(t = 6,0)$ их мощность перестает увеличиваться и начинает постепенно уменьшаться. Относительный размер антивирусной базы также постоянно уменьшается.

На рисунке 2 представлен модифицированный ответ ИИС с учетом кооперативного противостояния вторжению, следует отметить, что данные результаты можно интерпретировать, как пример – следующие начальные условия: относительная концентрация вируса – 1,0, относительная мощность антивируса – 0,5, относительный размер антивирусной базы – 0,3, поскольку ИИС-2 превентивно использует антивирусную базу ИИС-1 и поражаемый ресурс полностью свободен. Как видно из графиков (см. рисунок 2) при аналогичных начальных условиях (см. рисунок 1) иммунный ответ модифицированной ИИС, использующей сторонние антивирусные базы, в соответствии с выражением (2) становится более эффективным.

2. В данном случае ИИС, не подверженная атаке, передает второй ИИС в распоряжение не только свою, превентивно наращенную $C1^*(t)$, но и целиком свои антивирусные базы (см. рисунок 3).

Зависимости, приведенные на рисунке 3, характеризуют иммунный ответ ИИС на воздействие атаки в соответствии с выражением (2) при начальных условиях: относительная концентрация вируса – 1,0, относительная мощность антивируса – 0,5, относительный размер антивирусной базы – 0,0 и поражаемый ресурс полностью свободен. Как видно из графиков (см. рисунок 3), относительный объем антивирусной базы C стремительно растет и уже к $t = 14,0$ становится равным близко к единице, в свою очередь, это приводит к тому, что относительное количество вируса V начинает стремительно уменьшаться из-за работы антивирусных алгоритмов F, мощность которых, в свою очередь, сначала увеличивается до $t = 2,5,$ затем начинает плавно уменьшаться. После победы над вирусом

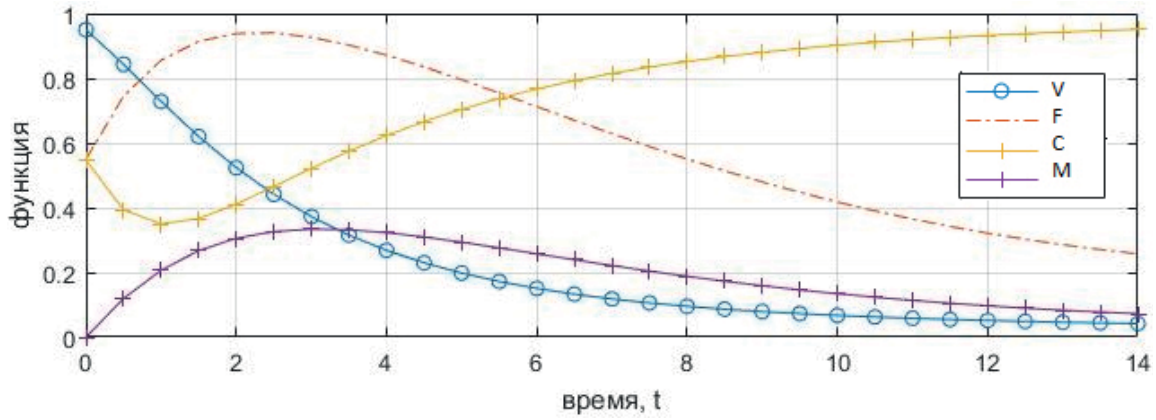

Рисунок 3. Результаты моделирования иммунного ответа ИИС с использованием сторонних антивирусных баз в полном объеме

накопленный объем антивирусной базы C может быть передан при необходимости следующей ИИС, находящейся под атакой.

3. В третьем случае возможно совместное использование антивирусных баз как первой, так и второй ИИС.

Для получения численного решения был проведен вычислительный эксперимент, в результате которого сформированы три основные стратегии иммунного ответа модифицированной ИИС при корпоративном противостоянии угрозам вторжения:

I – передача атакованной системе превентивно наращенной антивирусной базы $C_1^*(t)$ от «свободных» от атаки систем;

II – передача атакованной системе в полное распоряжение антивирусной базы «свободных» от атаки систем;

III – совместное использование антивирусных баз при атаках на обе ИИС.

При достаточно общей постановке задачи речь идет о необходимости выполнения кластеризации результатов наблюдений иммунного ответа ИИС на различные вирусные атаки. $O=\{O_1,\dots O_j,\dots,O_m\}$ – множество контролируемых ресурсов БТС. D_j – значение характеристики j-го ресурса БТС, векторная величина с компонентами элементов множеств O_j; V_j – скорость изменения значения D_j, векторная величина с компонентами элементов множеств O_j, где $V=\Delta V/\Delta t$; $\Delta V=D(t_i)-D(t_{i-1})$ – изменение значения D_j за время Δt; $\Delta t=t_i-t_{i-1}$ – промежуток между двумя соседними моментами времени; t_i – i-й момент времени измерения характеристик, $t_i\in[0;T]$.

В результате мы имеем три интервала, на которых определяются возможные состояния S_j^t.

Заключение

Таким образом, можно сделать вывод, что совместное использование антивирусных баз нескольких ИИС приводит к значительному повышению эффективности иммунного ответа. Модификация математических моделей иммунного ответа ИИС на внешнее вторжение с учетом накопления антивирусной базы с опережением $C^*(t)$ приносит положительный эффект в скорости уменьшения объемов накопленных вирусов $V^*(t)$ и повышении эффективности антивирусных алгоритмов $F^*(t)$.

Анализ полученных результатов приводит к выводу: модификация классических математических моделей в соответствии со спецификой ИИС значительно повысила их эффективность, что позволяет использовать методы ИИС для обнаружения уязвимостей интерфейсов БТС.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант № 19- 29-06015, 19-29-06023).

Литература

1. Detecting changes simulation of the technological objects' information states / A. Skatkov [et al.] // Proceedings of International Conference on Modern Trends in Manufacturing Technologies and Equipment (ICMTMTE 2018). 2018. Vol. 224. P. 02072. DOI: https://doi.org/10.1051/matecconf/201822402072
2. Дасгупта Д. Искусственные иммунные системы и их применение. М.: Физматлит, 2006. 344 с.
3. Скатков А.В., Брюховецкий А.А., Моисеев Д.В. Применение роевого интеллекта в задачах обнаружения аномалий состояний БТС // Сборник трудов VI Международной научно-практической конференции «Дистан-

ционные образовательные технологии». Симферополь: ИТ «АРИАЛ», 2021. С. 281–284.
4. Информационные технологии для критических инфраструктур: монография / под ред. А.В. Скаткова. Севастополь: СевНТУ, 2012. 306 с.
5. Брюховецкий А.А., Скатков А.В. Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем // Электротехнические и компьютерные системы. 2013. № 12 (88). С. 102–111.
6. A survey of artificial immune system based intrusion detection / H. Yang [et al.] // The Scientific World Journal. 2014. Vol. 2014, no. 156790.
7. Dasgupta D. Artificial Immune Systems and Their Applications. Moscow: Fizmatlit, 2006. 344 p.
8. Астахова И.Ф., Ушаков С.А. Модель и алгоритм искусственной иммунной системы // Математическое моделирование. 2016. Т. 28, № 12. С. 63–73.
9. Farmer J.D., Packard N., Perelson A. The immune system, adaptation and machine learning // Physica D: Nonlinear Phenomena. 1986. Vol. 2. P. 187–204.
10. Kephart J.O. A biologically inspired immune system for computers // Proceedings of Artificial Life IV: The Fourth International Workshop on the Synthesis and Simulation of Living Systems. 1994. P. 130–139.
11. Dasgupta D. Artificial Immune Systems and Their Applications. Berlin: SpringerVerlag, 1999. 320 p.
12. Скатков А.В., Брюховецкий А.А., Моисеев Д.В. Адаптация механизмов искусственных иммунных систем для контроля параметров окружающей среды // Системы контроля окружающей среды. 2020. № 2 (40). С. 127–133. DOI: https://doi.org/10.33075/2220-5861-2020-2-127-133
13. Skatkov A.V., Moiseev D.V., Bryukhovetskiy A.A. Model for vulnerabilities detection in unmanned vehicle interfaces based on artificial immune systems // Journal of Physics: Conference Series. 2020. No. 1515. P. 022043. DOI: https://doi.org/10.1088/1742-6596/1515/2/022043
14. Skatkov A.V., Bryukhovetskiy A.A., Moiseev D.V. Adaptive vulnerability detection model for unmanned vehicles drugs based on artificial immune systems // IOP Conference Series: Materials Science and Engineering. 2020. No. 734. P. 012028. DOI: https://doi.org/10.1088/1757-899X/734/1/012028
15. Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств: монография / А.В. Скатков [и др.]. Симферополь: ООО «Издательство Типография «Ариал», 2020. 352 с.
16. Мышкис А.Д. Линейные дифференциальные уравнения с запаздывающим аргументом. 2-е изд. М.: Наука, 1972. 352 с.
17. Цыпкин Я.З. Теория импульсных систем. М.: Государственное издательство физико-математической литературы, 1958. 724 с.
18. Каменский Г.А. К общей теории уравнений с отклоняющимся аргументом // Докл. АН СССР. 1958. Т. 120, № 4. С. 697–700.

Получено 16.12.2021

Скатков Александр Владимирович, д.т.н., профессор кафедры информационных технологий и компьютерных систем (ИТКС) Севастопольского государственного университета (СевГУ). 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 78408-84. E-mail: vml945@mail.ru

Моисеев Дмитрий Владимирович, д.т.н., профессор кафедры ИТКС СевГУ. 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 709-29-96. E-mail: dmitriymoiseev@mail.ru

Брюховецкий Алексей Алексеевич, к.т.н., доцент, заведующий кафедрой ИТКС СевГУ. 299053, Российская Федерация, г. Севастополь, ул. Университетская, 33. Тел. +7 978 811-62-46. E-mail: a.alexir@mail.ru

ADAPTATION OF MECHANISMS OF ARTIFICIAL IMMUNE SYSTEMS FOR COOPERATIVE RESISTANCE TO THREATS OF INTRUSION INTO AUTONOMOUS INFORMATION AND TELECOMMUNICATION FACILITIES

Skatkov A.V., Moiseev D.V., Bryukhovetsky A.A.

Sevastopol State University, Sevastopol, Russian Federation
E-mail: dmitriymoiseev@mail.ru

In this paper, the authors continue their research on the adaptation of the mechanisms of artificial immune systems by modifying classical mathematical models in accordance with the specifics of artificial immune systems, which allowed them to significantly increase their effectiveness in predicting the state of the object of control - solving the identification problem, which consists in finding the capacities of the sources of resource degradation (virus attack) of an autonomous information and telecommunications system according to available experimental data. The paper proposes models of cooperative interaction of several autonomous information and telecommunication systems, the protection of which is built on the basis of artificial immune systems. It is well-known that nowadays many methods based on the principles of immunology are expanding, and artificial immune systems are of the greatest interest among researchers due to the properties of special mechanisms of memory, search, recognition, adaptation, etc. The paper for the first time suggests the use of mechanisms for the transfer of antiviral databases between the artificial immune system of the donor and the artificial immune system of the acceptor. The results of a computational experiment are obtained, indicating the potential effectiveness of the proposed algorithms.

Keywords*: artificial intelligence, unmanned means of control, artificial immune systems, cooperative systems*

DOI: 10.18469/ikt.2021.19.4.04

Skatkov Alexander Vladimirovich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Professor, Doctor of Technical Science, Professor of Information Technology and Computer Systems Department. Tel. +7 978 784-08-84. E-mail: vml945@mail.ru

Moiseev Dmitriy Vladimirovich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Associate Professor, Doctor of Technical Science, Professor of Information Technology and Computer Systems Department. Tel. +7 978 709-29-96. E-mail: dmitriymoiseev@mail.ru

Bryukhovetskiy Alexey Alexeevich, Sevastopol State University, 33, Universetetskaya Street, Sevastopol, 299053, Russian Federation; Associate Professor, PhD in Technical Science, Head of Information Technology and Computer Systems Department. Tel. +7 978 811-62-46. E-mail: a.alexir@mail.ru

References

1. Skatkov A. et al. Detecting changes simulation of the technological objects' information states. *Proceedings of International Conference on Modern Trends in Manufacturing Technologies and Equipment (ICMTMTE 2018)*, 2018, vol. 224, pp. 02072. DOI: https://doi.org/10.1051/matecconf/201822402072
2. Dasgupta D. *Artificial Immune Systems and Their Applications*. Moscow: Fizmatlit, 2006, 344 p. (In Russ.)
3. Skatkov A.V., Bryukhovetskiy A.A., Moiseev D.V. The use of swarm intelligence in the tasks of detecting anomalies in the states of the BTS. *Sbornik trudov VI Mezhdunarodnoj nauchno-prakticheskoj konferentsii «Distantsionnye obrazovatel'nye tehnologii»*. Simferopol': IT «ARIAL», 2021, pp. 281–284. (In Russ.)
4. *Information Technologies for Critical Infrastructures: Monograph*. Ed. by A.V. Skatkov. Sevastopol': SevNTU, 2012, 306 p. (In Russ.)
5. Bryukhovetskiy A.A., Skatkov A.V. An adaptive model for intrusion detection in computer networks based on artificial immune systems. *Elektrotehnicheskie i komp'juternye si*stemy, 2013, no. 12 (88), pp. 102–111. (In Russ.)

6. Yang H. et al. A survey of artificial immune system based intrusion detection. *The Scientific World Journal*, 2014, vol. 2014, no. 156790,
7. Dasgupta D. *Artificial Immune Systems and Their Applications*. Moscow: Fizmatlit, 2006, 344 p.
8. Astahova I.F., Ushakov S.A. Model and algorithm of artificial immune system. *Matematicheskoe modelirovanie*, 2016, vol. 28, no. 12, pp. 63–73. (In Russ.)
9. Farmer J.D., Packard N., Perelson A. The immune system, adaptation and machine learning. *Physica D: Nonlinear Phenomena*, 1986, vol. 2, pp. 187–204.
10. Kephart J.O. A biologically inspired immune system for computers. *Proceedings of Artificial Life IV: The Fourth International Workshop on the Synthesis and Simulation of Living Systems*, 1994, pp. 130–139.
11. Dasgupta D. *Artificial Immune Systems and Their Applications*. Berlin: SpringerVerlag, 1999, 320 p.
12. Skatkov A.V., Bryukhovetskiy A.A., Moiseev D.V. Adaptation of the Mechanisms of Artificial Immune Systems to Control Environmental Parameters. *Sistemy kontrolja okruzhajuschej sredy*, 2020, no. 2 (40), pp. 127–133. DOI: https://doi.org/10.33075/2220-5861-2020-2-127-133 (In Russ.)
13. Skatkov A.V., Moiseev D.V., Bryukhovetskiy A.A. Model for vulnerabilities detection in unmanned vehicle interfaces based on artificial immune systems. *Journal of Physics: Conference Series*, 2020, no. 1515, pp. 022043. DOI: https://doi.org/10.1088/1742-6596/1515/2/022043
14. Skatkov A.V., Bryukhovetskiy A.A., Moiseev D.V. Adaptive vulnerability detection model for unmanned vehicles drugs based on artificial immune systems. *IOP Conference Series: Materials Science and Engineering*, 2020, no. 734, pp. 012028. DOI: https://doi.org/10.1088/1757-899X/734/1/012028
15. Skatkov A.V. et al. *Adaptive Vulnerability Detection of Unmanned Vehicle Interfaces: Monograph*. Simferopol': OOO «Izdatel'stvo Tipografija «Arial», 2020, 352 p. (In Russ.)
16. Myshkis A.D. *Linear Delay Differential Equations*. 2nd Ed. Moscow: Nauka, 1972, 352 p. (In Russ.)
17. Tsypkin Ya.Z. *Theory of Impulse Systems*. Moscow: Gosudarstvennoe izdatel'stvo fiziko-matematicheskoj literatury, 1958, 724 p. (In Russ.)
18. Kamenskij G.A. On the general theory of equations with deviating argument. *Dokl. AN SS*SR, 1958, vol. 120, no. 4, pp. 697–700. (In Russ.)

Received 16.12.2021

УДК 004.852

МНОГОШАГОВОЕ ПРОГНОЗИРОВАНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛОВ МОБИЛЬНОЙ СВЯЗИ 5G FR2

Трошин А.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: troshin-av@psuti.ru

Для использования всех возможностей мобильных сетей связи пятого поколения требуется освоение нового миллиметрового диапазона частот FR2, который ранее не применялся для мобильной связи. Его применение позволяет достигнуть максимальных скоростей доступа в сетях 5G, однако может приводить к сильным колебаниям пропускной способности каналов во времени. Для ряда мобильных приложений, таких как трансляция видео высокой четкости, может потребоваться адаптация к таким колебаниям на длительных временных интервалах. Такая адаптация возможна с использованием многошагового прогнозирования пропускной способности каналов 5G на основе предыдущих измерений и ряда других внешних факторов. Данная работа посвящена рассмотрению возможностей многошагового прогнозирования пропускной способности каналов 5G FR2 с использованием широкого круга моделей машинного обучения.

Ключевые слова: *5G, машинное обучение, многошаговое прогнозирование, нейронные сети*