УДК 681.3

***И.Г. Дровникова*[1], *Е.А. Рогозин*[1], *Д.И. Коробкин*[2], *А.А. Змеев*[3]**
([1]Воронежский институт МВД России, [2]ВУНЦ ВВС "ВВА",
[3]Военная академия ВКО им. Г.К. Жукова; e-mail: idrovnikova@mail.ru)

НОРМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ЭВОЛЮЦИОННОГО МОДЕЛИРОВАНИЯ

Приведены результаты нормирования требований к автоматизированным системам обеспечения техносферной безопасности с использованием эволюционного моделирования применительно к условиям подключения к сети "Интернет" в соответствии с базой данных реализации угроз безопасности информации.

Ключевые слова: *безопасность информации, генетический алгоритм, эволюционная модель.*

I.G. Drovnikova, E.A. Rogozin, D.I. Korobkin, A.A. Zmeev

SUBSTANTIATION NORMS OF SAFETY OF THE INFORMATION COMPUTING SYSTEMS WITH USE OF METHODS EVOLUTIONARY MODELLING

The results of the valuation requirements for automated systems to ensure safety technospheric using evolutionary momodeling applied to the conditions of connection to the network "Internet" in accordance with the database implementation of information security threats.

Key words: information safety, genetic algorithm, evolutionary model.

Статья поступила в редакцию Интернет-журнала 17 февраля 2015 г.

Обоснование требований к ***системам защиты информации (СЗИ)*** является одним из ключевых этапов проектирования АС в защищенном исполнении. Требования к СЗИ должны представлять собой количественные значения показателей защищенности информации от ***несанкционированного доступа (НСД)*** – норм безопасности информации. Разрабатываемая в настоящее время теория нормирования АС [1] основывается на решении оптимизационной задачи в следующей постановке.

Найти такой вектор значений показателей ИБ $\vec{K} = \langle k_1, k_2, ... k_p \rangle$, удовлетворяющий совокупности исходных данных $\{Y, \mathrm{O_s}, S, O_k, \Phi_c\}$ и обладающий при этом характеристикой наилучшего, в смысле выбранного критерия, предпочтения.

k_i – числовая характеристика защищенности, связанная с эффективностью ЗИ НСД монотонной зависимостью. Чем меньше k_i, тем лучше система при прочих равных условиях, то есть при неизменных $\{Y, \mathrm{O_s}, S, O_k, \Phi_c, \mathrm{O_э}\}$ и неизменных значениях остальных $m-1$ показателей качества защиты;

Y – совокупность условий применения СЗИ вида $Y = \{Y_1, Y_2, ... Y_l\}$;

O_s – совокупность ограничений на структуру параметры СЗИ НСД вида $O_s = \{O_{s1}, O_{s2}, ..O_{sq}\}$;

S – множество реализуемых или проектируемых СЗИ (вариантов построения системы) вида $S = \{S_1, S_2, ..S_d\}$.

d – допустимое множество СЗИ как существующих, так и перспективных;

O_k – ограничения на показатели качества $O_k = \{O_{k1}, O_{k2}, ..O_{kh}\}$. В случае выбора показателей качества в вероятностном виде ограничения принимают следующий вид: $0 < O_i < 1$ в виде диапазона;

Φ_c – векторная функция связи показателей числовых характеристик защищенности с эффективностью АС по прямому назначению.

В качестве целевой функции используется марковская модель защиты информации, моделирующая обобщенный алгоритм возникновения полного множества вариантов угроз НСД к информации в условиях реализации различных мер защиты информации [2, 3].

Модель защиты предназначена для оценки целевой функции ИБ – вероятности различных вариантов НСД и механизмов защиты в виде:

$$P_{нсд} = \prod_{i=1}^{3}(1-1/(1+\sum_{j=1}^{n,k,m}\frac{\lambda_i^j}{\mu_i^j}(1+\beta_i^j\frac{\mu_i^j}{\nu_i^j}))), \quad (1)$$

где i – этап возникновения НСД;

j – способ i-го этапа возникновения НСД имеет экспоненциальное распределение с параметром λ_{ij};

β_i^j – доля необнаруживаемых СЗИ типовых вариантов НСД для j-го способа i-го этапа рНСД;

ν_i^j – время задержки обнаружения скрытых действий по НСД j-го способа i –го этапа реализации угрозы;

μ_i^j – параметр экспоненциального времени нейтрализации обнаруженных действий j-го способа i-го этапа НСД;

n, k, m – количество способов НСД первого, второго и третьего этапов.

Значения λ_i^j определяются моделью полного множества вариантов НСД.

Анализ математического выражения (1) показал, что применение стандартных градиентных методов оптимизации затруднен в силу ряда особенностей этого математического выражения. В частности, оно имеет многопиковый вид, что приводит к проблемам преждевременной сходимости. Большое количество оптимизируемых переменных приводит к значительным вычислительным затратам.

В этой связи для решения задачи нормирования предлагается использовать методы эволюционного моделирования. В основе метода лежат ***генетические алгоритмы (ГА)*** [4, 5], являющиеся адаптивными алгоритмами оптимизации, использующими как аналог механизма генетического наследования, так и аналог естественного отбора.

В общем виде использование эволюционного моделирования для решения задачи нормирования можно представить в виде алгоритма, представленного на рис. 1.

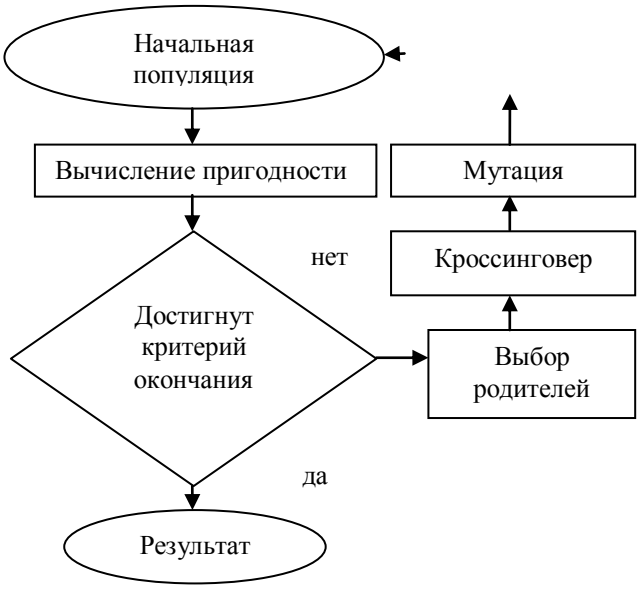

Рис. 1. Обобщенная схема генетического алгоритма

Генетические алгоритмы, по сравнению с градиентными методами оптимизации, обладают рядом преимуществ [4]:

- не требуют никакой информации о поведении функции (например, дифференцируемости и непрерывности);

- разрывы, существующие на поверхности ответа, имеют незначительное влияние на полную эффективность оптимизации;

- относительно стойки к попаданию в локальные оптимумы.

Решение задачи нормирования БИ АС с использованием модели защиты (1) эволюционного метода сводится к построению генетического алгоритма, представляющего структуру модели защиты [2], подобно тому, как ДНК (дезоксирибонуклеиновая кислота) представляет фенотипические свойства организма. При этом "хромосома" (генетический код) *s* эволюционной модели, используемой при нормировании требований к БИ АС, составляется в виде цепочек единиц и нулей, каждая из которых кодирует наличие или отсутствие одного из свойств модели защиты (2). Структура "хромосомы" процесса нормирования требований БИ АС представлена на рисунке 2 [4]. Поиск оптимальных решений заключается в поиске цепочек из всего их многообразия, обеспечивающих максимум функции приспособляемости.

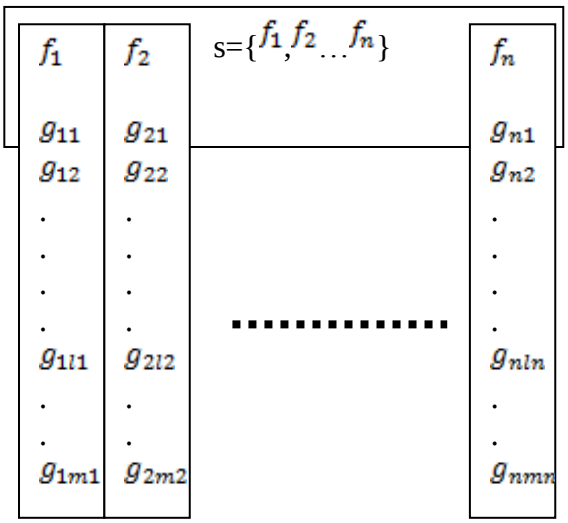

Рис. 2. Структура "хромосомы" генетического кода эволюционной модели нормирования требований к БИ АС

В соответствии с решаемой задачей нормирования требований к БИ АС, в качестве функции приспособляемости используется математическое выражение модели защиты (1).

В качестве исходных данных при проведении эволюционного моделирования целесообразно использовать данные, содержащиеся в наиболее известной общедоступной базе данных по НСД, накапливаемой DARPA (DARPA Intrusion Detection Attacks Database) [6]. Анализ данных позволил определить статистические характеристики НСД по данным записей эксперимента в виде, представленном в табл. 1.

Результаты проведения нормирования БИ АС с использованием эволюционного моделирования представлены на рис. 3-5. Для проведения эволюционного моделирования использовались встроенные функции построения ГА среды математических вычислений Mathlab.

На рис. 3 представлены значения нормированные характеристики СЗИ $\mu_1^1, \beta_1^1, \mu_1^2, \beta_1^2 \ldots \mu_3^6, \beta_3^6$, полученные с использованием эволюционного моделирования.

На рис. 4 представлено расстояние по Хеммингу между отдельными экземплярами СЗИ.

При проведении эволюционного моделирования использовались следующие параметры ГА:

- вероятность кроссинговера 80-95 %;
- вероятность мутации 0,5-1 %;
- размер популяции 100;
- рулеточный отбор новой популяции;
- критерий остановки численного эксперимента ГА окончание роста функции приспособляемости.

Таблица 1

Статистические характеристики реализации угроз БИ по данным записей эксперимента [6]

Наименование атаки	Вид параметров модели защиты	Параметр времени возникновения НСД v_i^j	Интенсивность возникновения λ_i^j
Сбор информации о топологии и принципах функционирования автоматизированной системы (Probes)			
Ipsweep	$v_1^1\ \lambda_1^1$	0,01	4,59e-6
Mscan	$v_1^2\ \lambda_1^2$	0,01	1,83e-7
Nmap	$v_1^3\ \lambda_1^3$	0,01	3,30e-6
Saint	$v_1^4\ \lambda_1^4$	0,01	3,67e-7
Satan	$v_1^5\ \lambda_1^5$	0,01	3,30e-6
Непосредственное проникновение в автоматизированную систему (Remote to Local User Attacks)			
Dictionary	$v_2^1\ \lambda_2^1$	0,001	9,18e-7
Ftpwrite	$v_2^2\ \lambda_2^2$	0,01	5,51e-7
Guest	$v_2^3\ \lambda_2^3$	0,01	7,34e-7
Imap	$v_2^4\ \lambda_2^4$	0,01	5,51e-7
Named	$v_2^5\ \lambda_2^5$	0,01	1,28e-6
Phf	$v_2^6\ \lambda_2^6$	0,01	5,51e-7
Sendmail	$v_2^7\ \lambda_2^7$	0,0001	3,67e-7
Xlock	$v_2^8\ \lambda_2^8$	0,001	3,67e-7
Xsnoop	$v_2^9\ \lambda_2^9$	0,01	3,67e-7
Установление контроля над автоматизированной системой (User to Root Attacks)			
Eject	$v_3^1\ \lambda_3^1$	0,001	8,45e-6
Ffbconfig	$v_3^2\ \lambda_3^2$	0,001	4,77e-6
Fdformat	$v_3^3\ \lambda_3^3$	0,001	3,49e-6
Perl	$v_3^4\ \lambda_3^4$	0,01	2,93e-6
Ps	$v_3^5\ \lambda_3^5$	0,01	7,34e-7
Xterm	$v_3^6\ \lambda_3^6$	0,01	5,51e-7

На рис. 5 представлено среднее и наилучшее значения функции приспособляемости (2) при эволюционном моделировании.

Таким образом, с использованием специального программного обеспечения, предназначенного для реализации ГА из состава среды математических вычислений Mathlab, проведено нормирование требований в соответствии с математической постановкой (1) применительно к модели защиты в виде математического выражения (2) и исходных данных, содержащихся в общедоступной базе данных по НСД, накапливаемой DARPA (табл. 1).

Использование эволюционного моделирования при проведении нормирования требований к БИ АС позволяет осуществить оптимизацию (2).

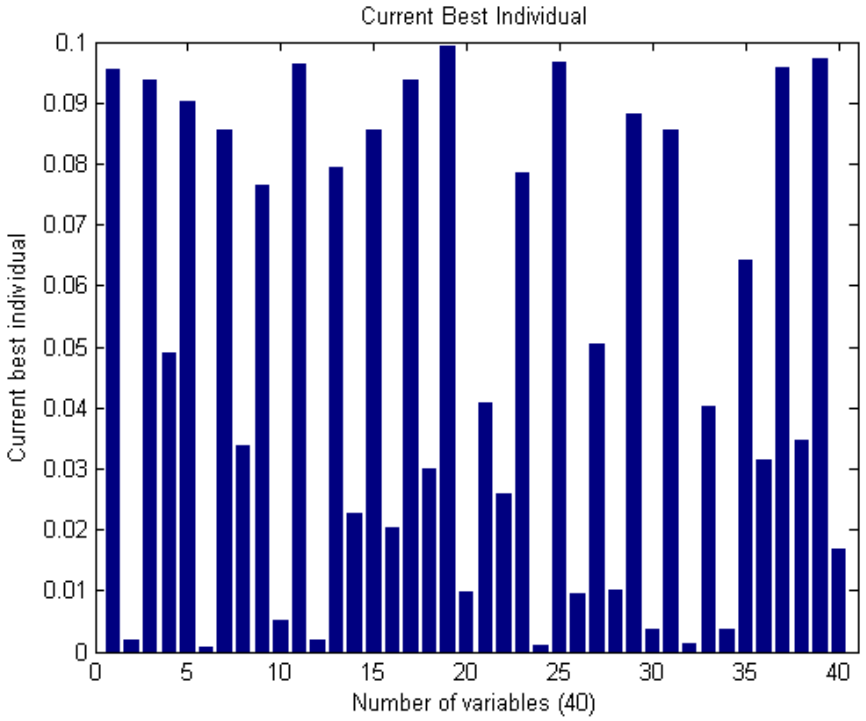

Рис. 3. Результаты нормирования требований к БИ АС
с использованием эволюционного моделирования

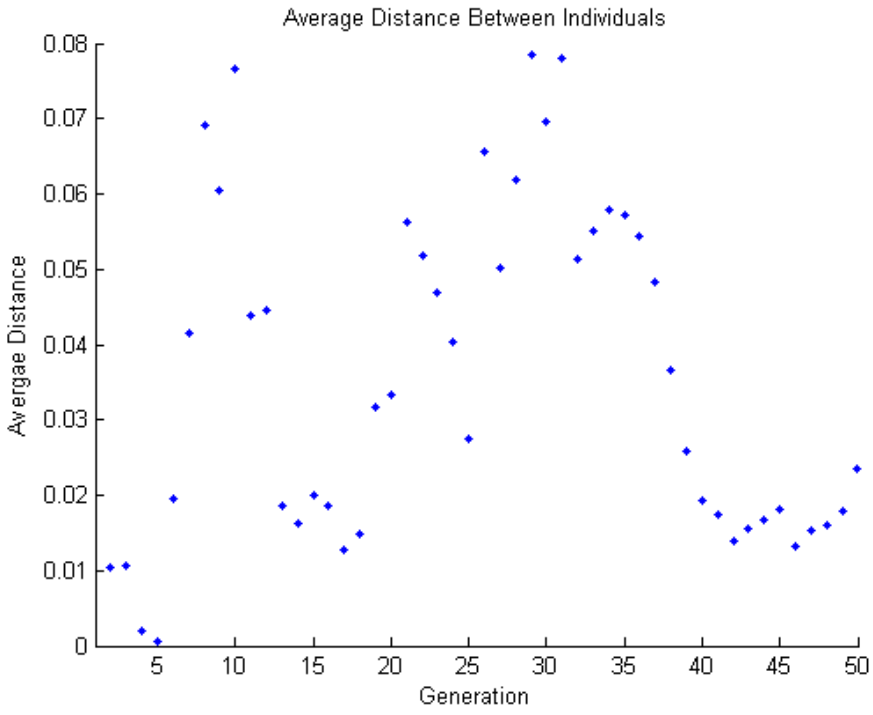

Рис. 4. Расстояние по Хеммингу между отдельными экземплярами СЗИ

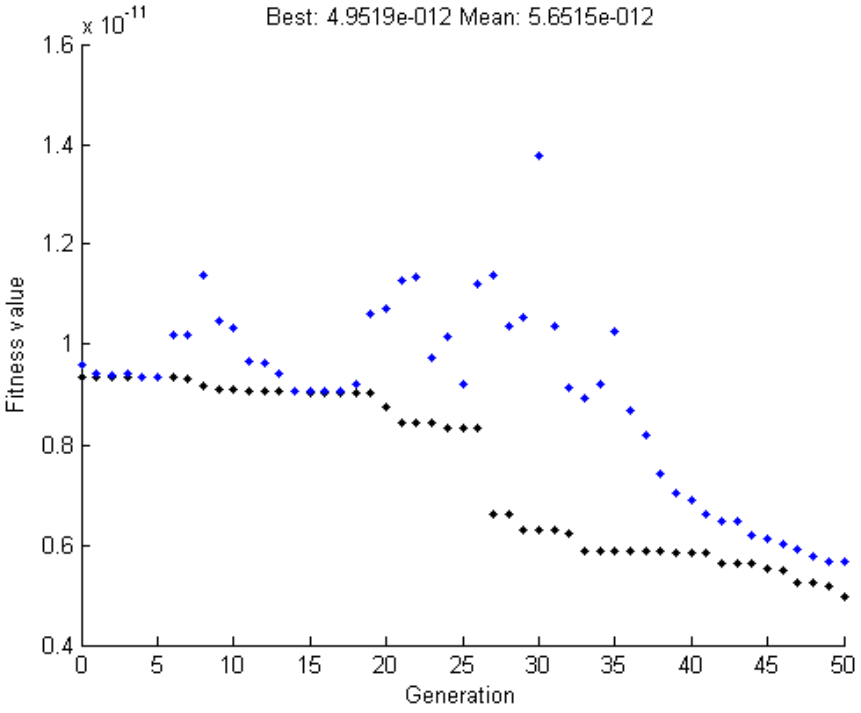

Рис. 5. Среднее и наилучшее значения функции приспособляемости (2) при эволюционном моделировании

Литература

1. ***Змеев А.А. и др.*** Методы и средства повышения защищенности автоматизированных систем: монография. Воронеж: Воронежский институт МВД России, 2013. 108 с.

2. ***Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А.*** Методика оценки вероятности несанкционированного доступа в автоматизированные системы, использующие протокол TCP/IP // Информация и безопасность. 2009. Т. 12. № 2. С. 285-288.

3. ***Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А.*** Об одном способе формализации понятия стойкости функции безопасности ГОСТ ИСО/МЭК 15408 // Вестник Воронежского государственного технического университета. 2009. Т. 5. № 2. С. 94-98.

4. ***Goldberg D.*** Genetic Algorithms in Search, Optimization, and Machine Learning. Massachusetts: Addison-Wesley, 1989.

5. ***Mitchell M.*** An Introduction to Genetic Algorithms. Cambridge: MIT Press, 1999. 158 c.

6. ***Cheung S., Lindqvist U., Fong M.*** Modeling Multistep Cyber Attacks for Scenario Recognition // Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III). Vol. 1, IEEE, 2003. Pp. 284-292.