ВЕСТНИК НОВЫХ МЕДИЦИНСКИХ ТЕХНОЛОГИЙ – 2014 – N 1
Электронный журнал

УДК 663.1:004.056 DOI: 10.12737/4108

ОБОСНОВАНИЕ НОРМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ЭВОЛЮЦИОННОГО МОДЕЛИРОВАНИЯ

В.П. ГУЛОВ[*], В.А. ХВОСТОВ[**], П.Е. ЧЕСНОКОВ[*]

[*]*ГБОУ ВПО ВГМА им. Бурденко Н.Н. Минздрава России, ул. Студенческая, д.10, г. Воронеж, Россия, 394000*

[**]*Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю», ул. 9 Января, д. 280а, г. Воронеж, Россия, 394026*

Аннотация. Проведен анализ проблемы обоснования норм безопасности информации медицинских информационных систем в виде количественных требований к показателям защищенности. Математическая постановка задачи нормирования требований к ним поставлена в виде оптимизационной задачи. На основе сравнительного анализа методов решения оптимизационных задач применительно к математическому выражению, формализующему модель защиты информации, предложен алгоритм нормирования, основанный на методах эволюционного моделирования защиты информации. Использование генетических алгоритмов для решения оптимизационных задач нормирования требований к безопасности информации позволяет преодолеть ряд проблем возникающих при применении градиентных методов в связи с многопиковым видом функции приспособливаемости и большим количеством оптимизируемых параметров. С использованием специального программного обеспечения из состава среды математических вычислений Matlab проведено нормирование требований к безопасности информации. В качестве исходных данных использованы стандартные данные, содержащиеся в наиболее известной общедоступной базе данных реализации угроз безопасности информации накапливаемой DARPA. Приведены результаты нормирования требований с использованием эволюционного моделирования при подключении к сети «Интернет» в соответствии со стандартными уровнями реализации угроз безопасности информации.

Ключевые слова: медицинская информационная система, генетический алгоритм, эволюционная модель, безопасность информации.

SUBSTANTIATION OF NORMS OF INFORMATION SAFETY OF MEDICAL INFORMATION SYSTEMS BY MEANS OF METHODS OF EVOLUTIONARY MODELLING

V.P. GULOV[*], V. A.KHVOSTOV[**], P.E. CHESNOKOV[*]

[*] *Medical University VGMA them. NN Burdenko Russian Ministry of Health, ul. Student, 10, Voronezh, Russia, 394000*

[**] *Federal Autonomous Institution "State Research and Testing Institute for technical protection of information from the Federal Service for Technical and Export Control," st. January 9, etc. 280a, Voronezh, Russia, 394026*

Abstract. The analysis of a problem a substantiation of norms of safety of medical information of information systems in the form of quantitative requirements to security indicators is carried out. Mathematical statement of a problem of rationing of requirements to safety of the information of medical information systems is put in the form of an optimizing problem. On the basis of the comparative analysis of methods of the decision of optimizing problems with reference to the mathematical expression formalizing model of protection of the information, the algorithm of rationing based on methods of evolutionary modeling of protection of the information in medical information systems is offered. Use of genetic algorithms for the decision of optimizing problems of rationing of requirements to safety of the information allows to overcome a number of problems arising at application gradient methods in connection with a multi-peak kind of function conforming and a considerable quantity of optimized parameters. With use of the special software intended for realization of genetic algorithms from structure of the environment of mathematical calculations Matlab rationing of requirements to safety of the information is spent. As initial data the standard data containing in the most known popular database of realization of threats of safety of the information accumulated DARPA are used. Results of rationing of requirements safety are led to the information of medical information systems with use of evolutionary modelling at connection to a network "Internet" according to standard levels of realization of threats of safety of the information.

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

В настоящее время в здравоохранении России в соответствии с федеральной целевой программой «Здравоохранение России» реализуются проекты по внедрению в поликлиниках и больницах электронных

медицинских карт пациентов, предоставлению услуг «электронной регистратуры», созданию территориальных медицинских регистров и *медицинских информационных систем* (МИС). Эта качественно новая технологическая среда информационного взаимодействия создает также и множество новых проблем, связанных с обеспечением конфиденциальности медицинской информации и сохранением врачебной тайны при их использовании [10-12].

Особую актуальность при реализации этих проектов приобретает проблема обеспечения защиты конфиденциальной информации в отношении специфичного класса защищаемой информации – *персональных данных* (ПДн), гарантия защиты которых закреплена законодательно [1, 2].

Обоснование требований к *системам защиты информации* (СЗИ) в целях *безопасности информации* (БИ) при обработке ПДн является одной из ключевых задач, решаемых при проектировании МИС. При этом последовательность создания СЗИ в МИС в интересах защиты информации при обработке ПДн определена в Методических рекомендациях Минздрава России [3].

Содержащиеся в [3] рекомендации по выполнению технических мероприятий по обеспечению безопасности ПДн разделяются на две категории. Обязательные технические мероприятия при реализации МИС любого класса и технические мероприятия, реализуемые при наличии соответствующего финансирования.

К первому классу относятся наиболее простые, но необходимые технические мероприятия по защите информации, такие как:

1. установка антивирусной защиты на все элементы МИС;
2. установка межсетевого экрана на границе сети;
3. использование криптозащиты.

Все остальные технические мероприятия, традиционно применяемые при решении задачи обеспечения БИ [4], относятся ко второму классу. При этом возможность их реализации в МИС в основном связана с объемом финансирования.

В этом случае актуальным является повышение защищенности информации МИС за счет целенаправленного объединении элементов СЗИ в систему. Последняя приобретает специфические свойства, изначально не присущие ни одной из ее составных частей. При системном подходе учитываются свойства СЗИ, которые определяют взаимодействие элементов друг с другом и оказывают влияние на АС в целом, а также на достижение поставленной цели безопасности.

Для этого показатели эффективности СЗИ должны представлять собой количественные значения показателей защищенности информации от *несанкционированного доступа* (НСД) – нормы безопасности информации. Разрабатываемая в настоящее время теория нормирования БИ МИС [4] основывается на решении оптимизационной задачи в следующей постановке.

Найти такой вектор значений показателей ИБ $\vec{K} = \langle k_1, k_2, ...k_p \rangle$, (1)

удовлетворяющего совокупности исходных данных $\{Y, \mathrm{O_s}, S, O_k, \Phi_c\}$ и обладающего 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, т. е. при неизменных $\{Y, \mathrm{O_s}, S, O_k, \Phi_c, \mathrm{O_э}\}$ и неизменных значениях остальных $m-1$ показателей качества защиты.

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

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

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 МИС по прямому назначению.

В качестве целевой функции, используется марковская модель защиты информации, моделирующая обобщенный алгоритм реализации полного множества угроз НСД к информации в условиях реализации различных мер по защите информации [5, 6].

Модель защиты предназначена для оценки целевой функции БИ – вероятности реализации различных вариантов угроз и механизмов защиты в виде: $P_{исд} = \prod_{i=1}^{3}(1 - 1/(1 + \sum_{j=1}^{n,k,m} \frac{\lambda_i^j}{\mu_i^j}(1 + \beta_i^j \frac{\mu_i^j}{\nu_i^j})))$ (2)

где i – этап реализации угрозы ИБ; j – способ i-го этапа реализации имеет экспоненциальное распределение с параметром λ_{ij}; β_i^j – доля не обнаруживаемых СЗИ типовых угроз ИБ для j-го способа i-го этапа реализации; 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 реализации угрозы; *n, k, m* – количество способов реализации угроз НСД первого, второго и третьего этапов.

Значения λ_i^j определяются моделью полного множества угроз БИ.

Анализ математического выражения (2) показал, что применение стандартных градиентных методов оптимизации затруднено в силу ряда особенностей этого математического выражения. В частности стандартные градиентные методы оптимизации не применимы к многопиковым функциям, к которым можно отнести математическое выражение (2), в связи с проблемой преждевременной сходимости. Также большое количество оптимизируемых переменных при использовании градиентных методов приводит к значительным вычислительным затратам.

В этой связи для решения задачи нормирования предлагается использовать методы эволюционного моделирования. В основе метода лежат *генетические алгоритмы* (ГА) [7, 8], являющиеся адаптивными алгоритмами оптимизации, использующими как аналог механизма генетического наследования, так и аналог естественного отбора.

ГА по сравнению с градиентными методами оптимизации обладают рядом преимуществ, например, такими как [7]:

1. не требуют никакой информации о поведении функции (например, дифференцируемости и непрерывности);
2. разрывы, существующие на поверхности ответа, имеют незначительный эффект на полную эффективность оптимизации;
3. относительно стойки к попаданию в локальные оптимумы.

Однако существует ряд трудностей в практическом использовании эволюционного моделирования, а именно, в многоэкстремальных задачах ГА сталкивается с множеством аттракторов.

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

Решение задачи нормирования БИ МИС с использованием модели защиты (1) с использованием эволюционного метода сводится к построению генетического кода, 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 МИС 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 МИС представлена на рис. 2 [7].

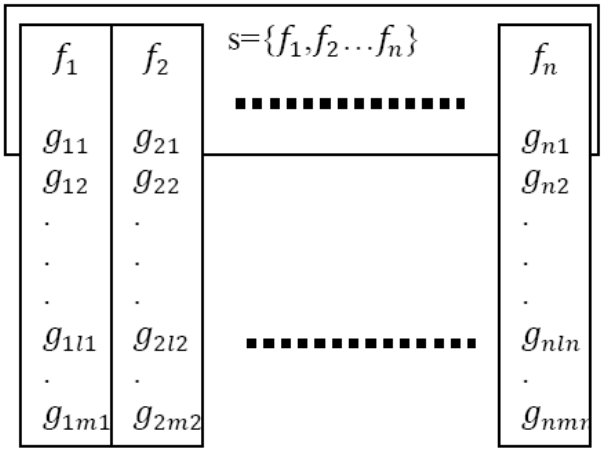

Рис. 2. Структура «хромосомы» генетического кода эволюционной модели нормирования требований к БИ МИС

Поиск оптимальных решений заключается в поиске цепочек из всего их многообразия, обеспечивающих максимум функции приспособливаемости.

В соответствии с решаемой задачей нормирования требований к БИ МИС в качестве функции приспособливаемости математическое выражение модели защиты (2).

В качестве исходных данных при проведении эволюционного моделирования целесообразно использовать стандартные данные, содержащиеся в наиболее известной общедоступной базе данных реализации угроз БИ накапливаемой DARPA (DARPA Intrusion Detection Attacks Database) [9]. Анализ данных позволил определить статистические характеристики реализации угроз БИ по данным записей эксперимента в виде, представленном в табл. 1.

Таблица 1

Статистические характеристики реализации угроз БИ по данным записей эксперимента [9]

№ п.п.	Наименование атаки	Вид параметров модели защиты	Параметр времени реализации	Интенсивность реализации
Сбор информации о топологии и принципах функционирования автоматизированной системы (Probes)				
1	Ipsweep		0.01	4,59e-6
2	Mscan		0.01	1,83e-7
3	Nmap		0.01	3,30e-6
4	Saint		0.01	3,67e-7
5	Satan		0.01	3,30e-6
Непосредственное проникновение в автоматизированную систему (RemotetoLocalUserAttacks)				
6	Dictionary		0.001	9,18e-7
7	Ftpwrite		0.01	5,51e-7
8	Guest		0.01	7,34e-7
9	Imap		0.01	5,51e-7
10	Named		0.01	1,28e-6
11	Phf		0.01	5,51e-7
12	Sendmail		0.0001	3,67e-7
13	Xlock		0.001	3,67e-7
14	Xsnoop		0.01	3,67e-7
Установление контроля над автоматизированной системой (UsertoRootAttacks)				
15	Eject		0.001	8,45e-6
16	Ffbconfig		0.001	4,77e-6
17	Fdformat		0.001	3,49e-6
18	Perl		0.01	2,93e-6
19	Ps		0.01	7,34e-7
20	Xterm		0.01	5,51e-7

Результаты проведения нормирования БИ МИС с использованием эволюционного моделирования представлены на рисунках 3-5. Для проведения эволюционного моделирования использовались встроенные функции построения ГА среды математических вычислений Matlab.

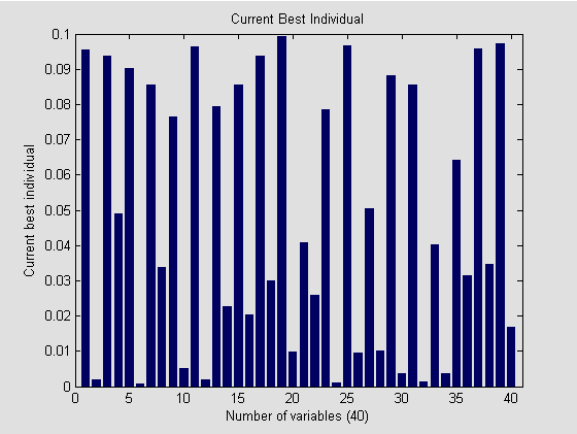

Рис. 3. Результаты нормирования требований к БИ МИС с использованием эволюционного моделирования

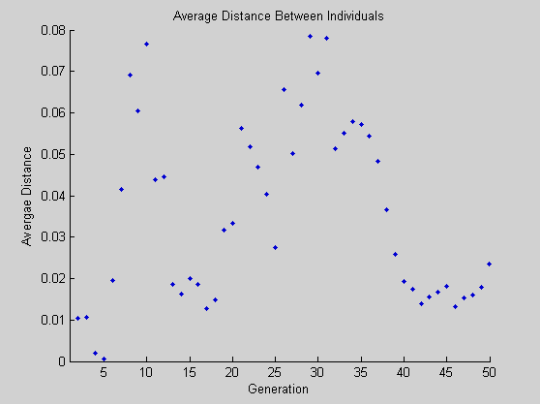

Рис. 4. Расстояние по Хеммингу между возможными вариантами СЗИ

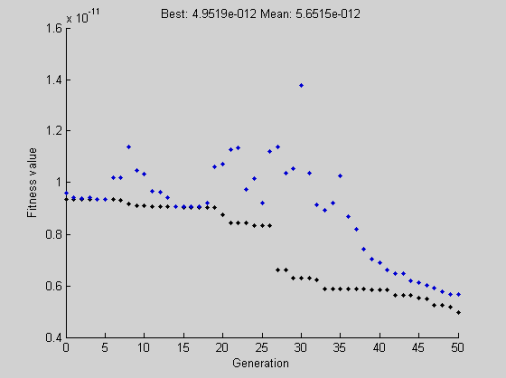

Рис. 5. Среднее и наилучшее значения функции приспособливаемости (2) при эволюционном моделировании

При проведении эволюционного моделирования использовались следующие параметры ГА:

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

На рис. 3 представлены значения нормированные характеристики СЗИ $x_1, x_2, x_3, \ldots, x_{40}$ полученные с применением эволюционного моделирования.

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

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

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

Использование эволюционного моделирования при проведении нормирования требований к БИ МИС позволяет осуществить оптимизацию (2) не смотря на многопиковый вид этого математического выражения, что приводит к проблемам преждевременной сходимости, а также его многомерный характер.

Литература

1. Федеральный закон N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» от 21 ноября 2011 г.

2. Федеральный закон «О персональных данных» № 152-ФЗ, от 27 июля 2006 года.

3. Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. Утверждены Министерством здравоохранения и социального развития РФ 23.12.2009 г., согласованы с ФСТЭК России.

4. Методы и средства повышения защищенности автоматизированных систем: монография / В.А. Хвостов [и др.]; под общ. ред. д-ра техн. наук, проф. С.В. Скрыля и д-ра техн. наук, проф. Е.А. Рогозина Воронеж: Воронежский институт МВД России, 2013 г. 108 с.

5. 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.

6. 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.

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

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

9. 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, 284–292.

10. Хадарцев А.А., Яшин А.А., Еськов В.М., Агарков Н.М., Кобринский Б.А., Фролов М.В., Чухраев А.М., Хромушин В.А., Гонтарев С.Н., Каменев Л.И., Валентинов Б.Г., Агаркова Д.И. Информационные технологии в медицине: Тула, 2006. 272 с.

11. Еськов В.М., Филатова О.Е., Фудин Н.А., Хадарцев А.А. Новые методы изучения интервалов устойчивости биологических динамических систем в рамках компартментно-кластерного подхода // Вестник новых медицинских технологий. 2004. Т. 11. № 3. С. 5.

12. Хромушин В.А., Хадарцев А.А., Хромушин О.В., Честнова Т.В. Обзор аналитических работ с использованием алгебраической модели конструктивной логики // Вестник новых медицинских технологий. (Электронное издание) 2011. №1. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2011-1/LitObz.pdf

Литература

1. Federal'nyy zakon N 323-FZ «Ob osnovakh okhrany zdorov'ya grazhdan v Rossiyskoy Federatsii» ot 21 noyabrya 2011 g. Russian.

2. Federal'nyy zakon «O personal'nykh dannykh» № 152-FZ, ot 27 iyulya 2006 goda. Russian.

3. Metodicheskie rekomendatsii po organizatsii zashchity informatsii pri obrabotke personal'nykh dannykh v uchrezhdeniyakh zdravookhraneniya, sotsial'noy sfery, truda i zanyatosti. Utverzhdeny Ministerst-vom zdravookhraneniya i sotsial'nogo razvitiya RF 23.12.2009 g., soglasovany s FSTEK Rossii. Russian.

4. Metody i sredstva povysheniya zashchishchennosti avtomatizirovannykh sistem: monografiya / V.A. Khvostov [i dr.]; pod obshch. red. d-ra tekhn. nauk, prof. S.V. Skrylya i d-ra tekhn. nauk, prof. E.A. Rogozina Voronezh: Voronezhskiy institut MVD Rossii; 2013. Russian.

5. Kislyak AA, Makarov OYu, Rogozin EA, Khvostov VA. Metodika otsenki veroyatnosti nesanktsionirovannogo dostupa v avtomatizirovannye sistemy, ispol'zuyushchie protokol TCP/IP. Informatsiya i bezo-pasnost'. 2009;12(2):285-8. Russian.

6. Kislyak AA, Makarov OYu, Rogozin EA, Khvostov VA. Ob odnom sposobe formalizatsii ponyatiya stoykosti funktsii bezopasnosti GOST ISO/MEK 15408. Vestnik Voronezhskogo gosudarstvennogo tekhni-cheskogo universiteta. 2009;5(2):94-8. Russian.

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

8. Mitchell M. An Introduction to Genetic Algorithms. Cambridge: MIT Press; 1999.

9. 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.

10. Khadartsev AA, Yashin AA, Es'kov VM, Agarkov NM, Kobrinskiy BA, Frolov MV, Chukhraev AM, Khromushin VA, Gontarev SN, Kamenev LI, Valentinov BG, Agarkova DI. Informatsionnye tekhnologii v meditsine: Tula; 2006. Russian.

11. Es'kov VM, Filatova OE, Fudin NA, Khadartsev AA. Novye metody izucheniya intervalov ustoy-chivosti biologicheskikh dinamicheskikh sistem v ramkakh kompartmentno-klasternogo podkhoda [New methods of investigation of biological dynamic systems' stability according to compartmental-cluster approach]. Vestnik novykh meditsinskikh tekhnologiy. 2004;11(3):5. Russian.

12. Khromushin VA, Khadartsev AA, Khromushin OV, Chestnova TV. Obzor analiticheskikh rabot s ispol'zovaniem algebraicheskoy modeli konstruktivnoy logiki [The review of analytic works with the application of constructive logic model development]. Vestnik novykh meditsinskikh tekhnologiy. (Elektronnoe izdanie) [Internet]. 2011 [cited 2011 Aug 16];1:[about 4 p.]. Russian. Available from: http://www.medtsu.tula.ru/VNMT/ Bulletin/E2011-1/LitObz.pdf