Для цитирования: *Дровникова И.Г., Змеев А.А., Рогозин Е.А. Частная методика формирования требований к системам защиты информации от несанкционированного доступа в автоматизированные системы с использованием генетического алгоритма. Вестник Дагестанского государственного технического университета. Технические науки. 2018; 45(3): 114-122. DOI:10.21822/2073-6185-2018-45-3-114-122*

For citation: *Drovnikova I.G., Zmeev A.A., Rogozin E.A. Private technique of formation of requirements to information protection systems from unauthorized access to automated bath systems using genetic algorithm. Herald of Daghestan State Technical University. Technical Sciences. 2018; 45(3): 114-122. (In Russ.) DOI:10.21822/2073-6185-2018-45-3-114-122*

ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.3
DOI: 10.21822/2073-6185-2018-45-3-114-122

ЧАСТНАЯ МЕТОДИКА ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКОГО АЛГОРИТМА

Дровникова И.Г.[1], Змеев А.А.[2], Рогозин Е.А.[3]
[1,3] Воронежский институт Министерства внутренних дел Российской Федерации,
[1,3]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2]Военная академия воздушно-космической обороны им. Г.К. Жукова,
[2]170022, Россия, г. Тверь, ул. Жигарева, 50, Россия,
[1]e-mail:idrovnikova@mail.ru, [2]e-mail tzmeev@yandex.ru, [3]e-mail evgenirogozin@yandex.ru

Резюме. Цель. *Анализ существующей методики формирования требований к системам защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированные системы (АС) выявил ряд существенных недостатков, основным из которых является следующий: несмотря на то, что рассматриваемая методика, несомненно, обладает теоретической значимостью, в то же время, она не может претендовать на практическую ценность. Это связано с тем, что в указанной методике исследования проводились не на конкретной типовой (широко используемой сертифицированной согласно нормативным документам Федеральной службы по техническому и экспортному контролю России) СЗИ, и приведённые в ней данные по угрозам НСД не соответствуют реальности (морально устарели), а, следовательно, требуют существенного обновления. Приняв существующую методику в качестве базовой, целью статьи является разработка частной методики формирования требований к СЗИ от НСД в АС, обладающей практической ценностью и позволяющей формировать количественные требования к широкому классу сертифицированных СЗИ.* ***Метод.*** *При написании статьи использованы методы системного анализа, эволюционного моделирования, теории вероятностей и математической статистики, математического аппарата для моделирования динамических дискретных сетей (Е-сетей), теории алгоритмов. Методологической основой является системный подход.* ***Результат.*** *Разработана частная методика, определяющая параметры символьного генетического алгоритма (ГА) для создания программного комплекса анализа, эволюционного моделирования и формирования количественных требований к СЗИ от НСД в АС при использовании возможностей пакета прикладных программ Matlab 13 для реализации ГА в среде программирования* Optimization toolbox. ***Вывод.*** *Предложенная частная методика формирования требований к СЗИ от НСД в АС с использованием ГА обладает теоретической значимостью, практической ценностью и позволяет формировать количественные требования к широкому классу сертифицированных по определённому классу защищённости АС в соответствии требованиями действующей нормативной документации.*

Ключевые слова: *автоматизированная система, система защиты информации, несанкционированный доступ, генетический алгоритм, оценочная сеть (Е-сеть), марковская модель*

TECHNICAL SCIENCE
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

PRIVATE TECHNIQUE OF FORMATION OF REQUIREMENTS TO INFORMATION PROTECTION SYSTEMS FROM UNAUTHORIZED ACCESS TO AUTOMATED BATH SYSTEMS USING GENETIC ALGORITHM

Irina G. Drovnikova[1], Anatoly A. Zmeev [2], Evgenii A. Rogozin[3]
[1,3]Voronezh Institute of the Ministry of the Interior of the Russian Federation,
[1,3]53 Patriotov Str., Voronezh 394065, Russia,
[2]G.K. Zhukov Military Academy of Aerospace Defense,
[2]50 Zhigareva Str., Tver, 2170022, Russia,
[1]e-mail:idrovnikova@mail.ru, [2]e-mail tzmeev@yandex.ru, [3]e-mail evgenirogozin@yandex.ru

Abstract. Objectives *Analysis of the existing methodology for the formation of requirements for information protection systems (GIS) from unauthorized access (NSD) to automated systems (AS) revealed a number of significant flaws, the main of which is the following: despite the fact that the considered method undoubtedly has theoretical significance, the same time, it can not claim practical value. This is due to the fact that in this methodology, the studies were carried out not on a specific standard (widely used certified according to the regulations of the Federal Service for Technical and Export Control of Russia) GIS, and the data on threats of unauthorized access given in it do not correspond to reality (morally obsolete), but therefore require a significant upgrade. Accepting the existing methodology as a baseline, the purpose of the article is to develop a private method of forming requirements for GIS from unauthorized access to the AU, which has practical value and allows you to formulate quantitative requirements for a wide class of certified GIS.* ***Method.*** *When writing the article, the methods of system analysis, evolutionary modeling, probability theory and mathematical statistics, mathematical apparatus for modeling dynamic discrete networks (E-networks), and theory of algorithms were used. The methodological basis is a systematic approach.* ***Result.*** *A private methodology has been developed that determines the parameters of the symbolic genetic algorithm (GA) for creating a software package for analysis, evolutionary modeling, and forming quantitative requirements for GIS from unauthorized access to speakers using the Matlab 13 application software to implement GA in the Optimization toolbox programming environment.* ***Conclusion.*** *The proposed private method of forming requirements for GIS from unauthorized access in the AU using GA has a theoretical significance, practical value and allows you to formulate quantitative requirements for a wide class of AS certified in a certain class of security in accordance with the requirements of current regulatory documentation.*

Keywords: *automated system, information protection system, unauthorized access, genetic algorithm, evaluation network (E-network), Markov model*

Введение. Опыт эксплуатации современных АС показал, что наибольший вклад в снижение их надёжности и работоспособности вносят факторы, связанные с НСД к информационному ресурсу этих систем [1, 2]. В соответствии с руководящими документами ФСТЭК России [3] основным элементом противодействия угрозам НСД в АС является СЗИ от НСД. Следовательно, ключевым вопросом современной теории защиты информации (ЗИ) от НСД в АС является формирование требований к СЗИ данных систем.

Одним из перспективных направлений решения этой сложной проблемы рассматривается использование методов эволюционного моделирования, реализованное в конкретную методику, представленную в [2]. Её анализ показал, что данная методика, несомненно, обладает теоретической значимостью, однако вопросы, связанные с её практической ценностью, исследованы в недостаточном объёме и нуждаются в существенной доработке. Следовательно, приняв существующую методику в качестве основной (базовой), необходимо разработать частную методику, обладающую практической значимостью и позволяющую формировать количественные требования к широкому классу сертифицированных СЗИ от НСД в АС, чему и посвящена данная статья.

Постановка задачи. Для устранения имеющихся недостатков базовой методики в процессе разработки частной методики можно выделить следующие основные направления исследований:

1. Анализ существующих широко используемых сертифицированных СЗИ от НСД с целью создания их вербальной модели, лежащей в основе построения формальной модели процесса функционирования этих систем с использованием оценочных сетей (Е-сетей).

2. На основе теории марковских процессов создание математической модели процесса функционирования защищённой АС, позволяющей получить адекватную модель случайных процессов, которую можно использовать в качестве основы целевой функции (функции приспособленности) решения задачи оптимизации параметров и характеристик функционирования СЗИ от НСД в АС.

3. По результатам анализа [1, 4] определение наиболее опасных угроз НСД с точки зрения последствий их реализации в АС и разработка графовых моделей данных деструктивных воздействий, которые послужат основой для исследования их вероятностно-временных характеристик (значений средних времён нахождения каждой из угроз в одном из состояний графовой модели) в программной среде имитационного моделирования CPN Tools.

4. Определение параметров символьного ГА (размера популяций, типа селекции, генетических операторов и их вероятностей, величины разрыва поколений) для разработки программного комплекса анализа, эволюционного моделирования и формирования количественных требований к СЗИ от НСД в АС при использовании возможностей пакета прикладных программ Matlab 13 для реализации ГА в среде программирования Optimization toolbox.

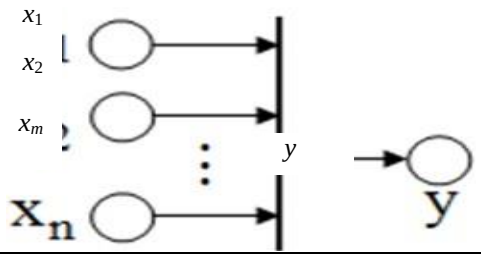
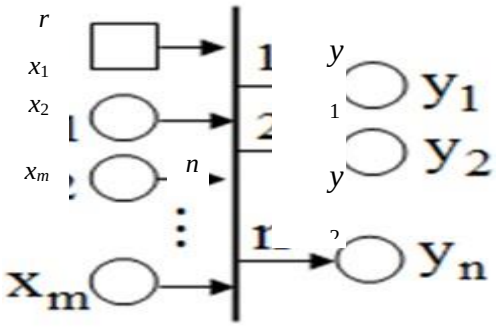
Методы исследования. Для проведения исследований необходимо по результатам анализа [3] построить вербальную модель широко используемой сертифицированной СЗИ от НСД «Dallas lock», которая устанавливается на ПЭВМ, работающих под управлением операционных систем семейств Windows и Linux. При разработке АС в защищённом исполнении данная СЗИ от НСД имеет сертификат по 1Б, 1В, 1Г, 1Д, 2А, 2Б, 3А, 3Б классам защищённости. «Dallas lock» используется как в государственных, так и в коммерческих структурах, имея множество сертификатов совместимости с другими программными продуктами.

«Dallas lock» включает в себя шесть подсистем обеспечения ЗИ в АС [2]: самодиагностики, управления доступом, администрирования параметров СЗИ от НСД, идентификации и аутентификации пользователей, контроля целостности рабочей среды пользователей АС, регистрации и учёта. При проведении и анализе современных исследований процесса функционирования сложных систем [2], к которым, безусловно, следует отнести и СЗИ от НСД, рекомендуется использовать методы математического моделирования.

Одним из основных этапов, определяющих качество создания математической модели СЗИ от НСД в АС, является формализация процесса функционирования данной СЗИ. Перспективным подходом к построению формальной модели процесса функционирования СЗИ от НСД является представление этого процесса в виде ориентированного графа [4]. Ориентированный граф также можно рассматривать как общий математический объект, специально не предназначенный для создания модели функционирования СЗИ от НСД в её динамике. Следовательно, с целью формализованного описания СЗИ от НСД в виде ориентированного графа необходимо в рамках графового подхода разработать частные математические объекты данной модели. Анализ подобных математических объектов позволил для разработки математической модели динамики функционирования СЗИ от НСД в АС использовать оценочные сети (Е-сети), являющиеся дальнейшим развитием сетей Петри [5 – 7].

Процесс построения оценочной сети подробно изложен в [6, 7], поэтому его теоретическая часть в данной статье не приводится. Основные элементарные сети формального описания процесса функционирования СЗИ от НСД в АС, состоящие из 2 видов оценочных сетей – сети типа *J* (объединение) и сети типа *X* (переключатель), представлены в табл. 1, где r, x_i, y_j – соответственно разрешающая, входная и выходная позиции объекта (состояния функционирования СЗИ от НСД); $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, n$; m и n – соответственно количество входных и выходных позиций.

Таблица 1. Основные элементарные сети формального описания процесса функционирования СЗИ от НСД в АС
Table 1. The main elementary networks of the formal description of the process of functioning of GIS from unauthorized access to the AU

Тип перехода Type of transition	Графическое представление Graphic representation	Условное обозначение Conventional symbol
Объединение Union		$J\ (x_1, x_2, \ldots, x_m, y)$
Переключатель Switch		$X\ (r, x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n)$

На рис. 1 изображена оценочная сеть процесса функционирования широко используемой сертифицированной СЗИ от НСД «Dallas lock». Нахождение СЗИ от НСД в простой позиции определяет выполнение функции ЗИ, номер которой обозначен в кружочке, отображающем данную позицию.

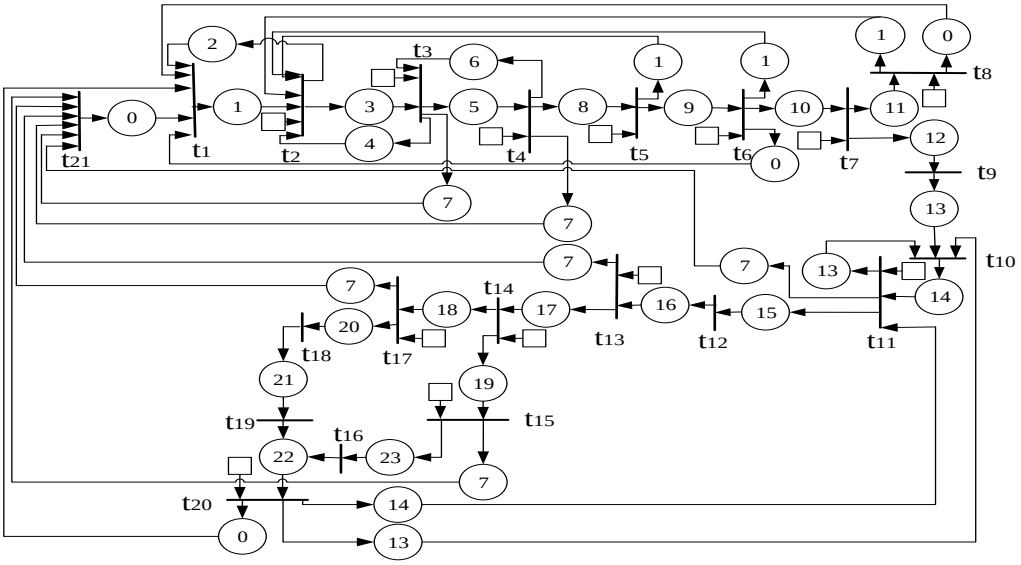


Рис. 1. Оценочная сеть процесса функционирования широко используемой сертифицированной СЗИ от НСД «Dallas lock»
Fig. 1. Evaluation network of the widely used certified DSS from the unauthorized access control system "Dallas lock"

Таблица 2. Сведения о сервисных функциях ЗИ с временами их выполнения (в секундах) и соответствующими элементарными сетями, отображающих функционирование СЗИ от НСД «Dallas lock»

Table 2. Information about the information protection service functions with the time of their execution (in seconds) and the corresponding elementary networks that display the functioning of the information protection system against unauthorized access "Dallas lock"

Номер и наименование функции СЗИ от НСД Number and name of the function information security systems against unauthorized access	Номер перехода Transition number	Элементарная сеть Elementary network
1. Ввод имени пользователя (авторизация). Enter user name (authorization)	t_1	$J\,(x_0, x_0, x_0, x_0, x_0, x_2, y_1)$
2. Повторный ввод имени пользователя. Re-enter username	t_2	$X\,(r_1, x_1, x_1, x_1, x_1, x_4, y_2, y_3)$
3. Ввод пароля. Password entry	t_3	$X\,(r_2, x_3, x_6, y_4, y_5, y_7)$
4. Повторный ввод пароля. Re-enter password	t_4	$X\,(r_2, x_3, y_6, y_7, y_8)$
5. Ввод идентификатора. ID entry	t_5	$X\,(r_4, x_8, y_1, y_9)$
6. Повторный ввод идентификатора. Re-enter id	t_6	$X\,(r_4, x_8, y_1, y_9)$
7. Блокировка в случае неоднократно неправильно введённого пароля, несоответствия пользователя и предъявляемого идентификатора. Blocking in case of repeatedly incorrectly entered password, user mismatch and identifier being shown	t_7	$X\,(r_5, x_{10}, y_{11}, y_{12})$
8. Проверка доступного времени работы пользователя Check available user time	t_8	$X\,(r_6, x_{11}, y_0, y_1)$
9. Контроль доступа Access control	t_9	$J\,(x_{12}, y_{13})$
10. Проверка срока действия пароля Verify password expiration	t_{10}	$J\,(x_{13}, x_{13}, x_{13}, y_{14})$
11. Разрешений на изменение пароля Password change permissions	t_{11}	$X\,(r_7, x_{14}, x_{14}, y_7, y_{13}, y_{15})$
12. Вход в систему Login to the system	t_{12}	$J\,(x_{15}, y_{16})$
13. Обращение к ресурсу Addressing a resource	t_{13}	$X\,(r_8, x_{16}, y_7, y_{17})$
14. Мандатный механизм управления доступом. Соотносятся метки конфиденциальности пользователя и ресурса. Mandatory access control mechanism. Associate user privacy and resource labels	t_{14}	$X\,(r_9, x_{17}, y_{18}, y_{19})$
15. Обращение к объекту Appeal to the object	t_{15}	$X\,(r_{10}, x_{17}, y_7, y_{23})$
16. Проверка полномочий доступа пользователя, основанного на дискреционном принципе контроля доступа Authorization of user access based on discretionary principle of access control	t_{16}	$J\,(x_{23}, y_{22})$
17. Допуск субъекта к защищаемому объекту The subject's admission to the protected object	t_{17}	$X\,(r_{11}, x_{18}, y_7, y_{23})$
18. Запрос на преобразование объекта. Request for object conversion	t_{18}	$J\,(x_{20}, y_{21})$
19. Запрос на удаление Request for deletion	t_{19}	$J\,(x_{21}, y_{22})$
20. Преобразование объекта перед удалением Convert the object before deleting	t_{20}	$X\,(r_{22}, x_{18}, y_0, y_{13}, y_{14})$
21. Удаление объекта Deletion of an object		
22. Завершение работы с объектом Completion of work with the object	t_{21}	$J\,(x_7, x_7, x_7, x_7, x_7, x_7, y_0)$
23. Пересчёт параметров целостности объекта Recalculation of the parameters of the integrity of the object		

В табл. 2 представлены функции ЗИ с временами их выполнения (в секундах) и соответствующими элементарными сетями.

Случайные переходы между состояниями функционирования СЗИ от НСД реализуются разрешающими процедурами. Данные переходы принято считать равновероятными, т.е. вероятность P_{ij} перехода из состояния i в последующее за ним состояние j равна $P_{ij} = 1/K$, где K – общее количество переходов из состояния i.

С целью оценки эффективности функционирования типовой СЗИ от НСД «Dallas lock» проведём анализ разработанной оценочной сети, приведённой на рис. 1, с использованием основных положений теории марковских процессов [8, 9]. Поскольку оценочная сеть представляет собой случайный марковский процесс с конечным числом состояний (марковскую цепь), то в соответствии с [8] время пребывания системы в одном из состояний апроксимируется экспоненциальным законом распределения.

Полагаем, что основные функции СЗИ от НСД будут реализованы в АС, если время $\tau_{инт}$ (время выполнения основных функциональных задач СЗИ от НСД) не превышает значения максимально допустимого времени τ_{max}, приведённого в технической документации на защищённую АС в разделе «Защита информации от НСД» [3].

Учитывая, что процесс функционирования СЗИ от НСД представляет собой случайный процесс, формула для оценки эффективности функционирования этих систем примет вид [9] $K_{эф} = P(\tau_{инт} \le \tau_{max})$, где: $K_{эф}$ – показатель временной эффективности программных систем (т.е. способность СЗИ от НСД выполнять заданные действия в интервале времени, отвечающем заданным требованиям), позволяющий описывать защищённость АС; P – вероятность своевременного выполнения СЗИ декларированных функций.

Из [8] известно, что марковский процесс с конечным числом состояний описывается матрицей вероятностей переходов СЗИ от НСД в одно из состояний $n = \overline{1,27}$.

Далее определяется система уравнений, представляющая собой расчёт переходных вероятностей, которая стандартным образом [10] может быть решена итерационным методом Зейделя, подробно изложенным в [8]. Достоинство предложенного метода состоит в простоте его алгоритма, самоуправляемости и удобстве реализации, экономичности с точки зрения необходимой памяти при проведении расчётов по сравнению с методами Гаусса и Гивенса. Недостатком метода является его возможная расходимость [8].

Алгоритм для оценки показателя эффективности функционирования СЗИ от НСД «Dallas lock» на основе использования итерационного метода Зейделя представлен на рис. 2.

Описание работы алгоритма:

1 – сбор информации о функционировании СЗИ от НСД, а именно получение статистических данных о работе каждой её составной части при помощи программных или технических средств;

2 – ввод полученных данных в программный комплекс с целью оценки эффективности исследуемой СЗИ от НСД;

3 – определение среднего времени ожидания выполнения функцией СЗИ от НСД возложенных на неё задач при реализации ЗИ в АС;

4 – преобразование Лапласа для получения системы линейных алгебраических уравнений;

5, 6, 7 – перебор всех полученных значений и выполнение преобразования Лапласа для получения системы линейных алгебраических уравнений;

8 – задание требуемой точности e и e_{max} равной нулю для того, чтобы на последующих этапах сразу не закончилось прохождение по алгоритму;

9, 10, 11 – проверка условия сходимости: если i не равно j, то необходимо и достаточно, чтобы все собственные значения матрицы были по модулю меньше единицы; тогда продолжается движение по алгоритму, в противном случае – условие не выполнено;

12 – проверка условия: если требуемая точность меньше, то считается, что найдены значения всех неизвестных в системе линейных алгебраических уравнений; в противном случае поиск нужных значений продолжается;

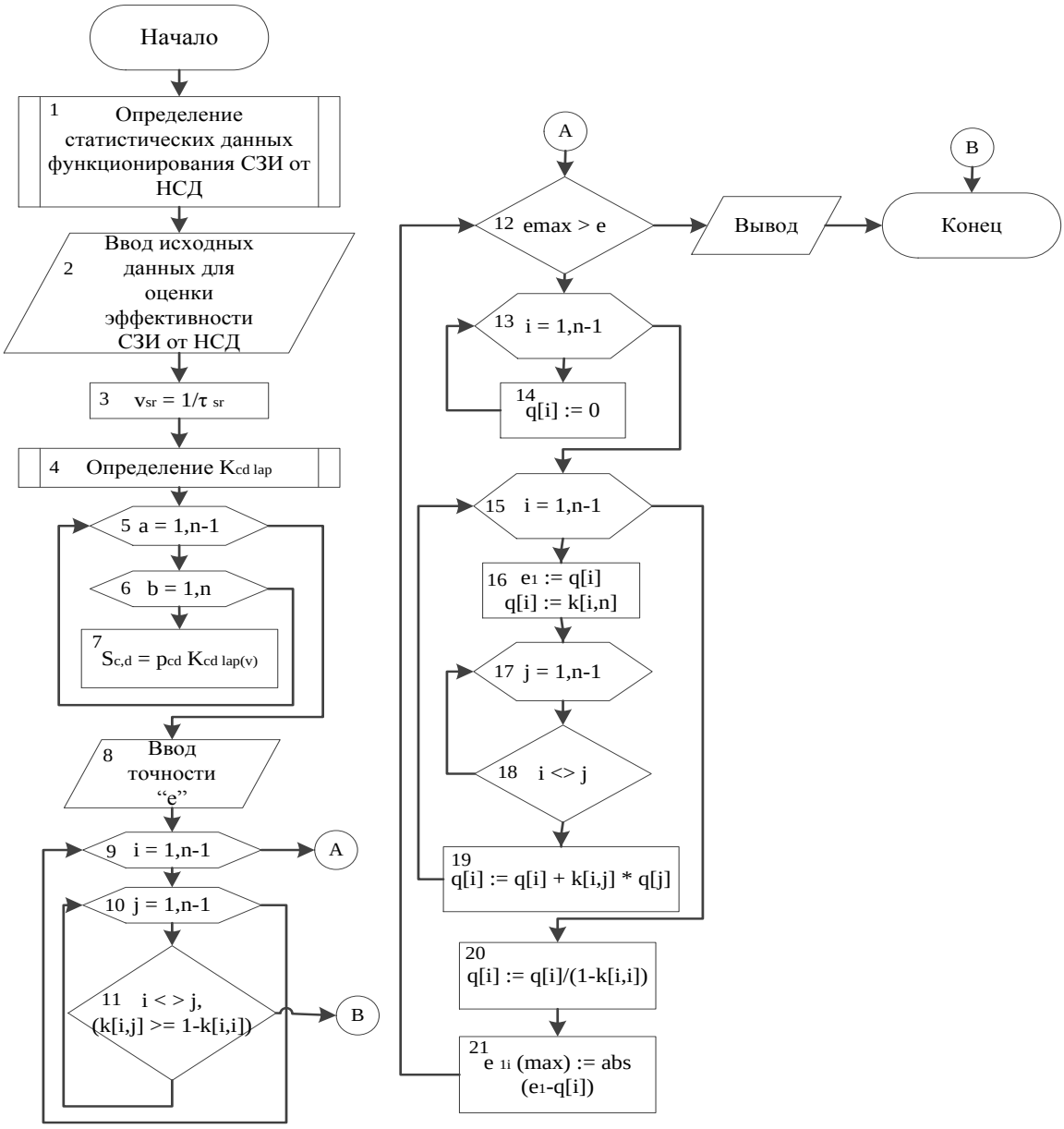


Рис. 2. Алгоритм оценки показателя эффективности функционирования СЗИ от НСД «Dallas lock» на основе итерационного метода Зейделя
Fig. 2. Algorithm for evaluating the performance of the information security system from unauthorized access "Dallas lock" based on the iterative method of Seidel

13, 14 – задание начального вектора q_i;

15, 16, 17, 18, 19 – подсчёт значений неизвестных на текущей итерации: если i не равно j, то используются значения, либо полученные ранее, либо подсчитанные на этой итерации;

20 – деление на коэффициент при i-ой неизвестной;

21 – подсчёт абсолютной величины разности между элементами предыдущего и текущего шагов.

Обсуждение результатов. В настоящее время создание методики формирования количественных параметров (характеристик) эффективности функционирования существующих и перспективных (разрабатываемых) СЗИ от НСД в АС является довольно сложной и актуальной проблемой.

Это связано с тем, что существующая методика формирования требований к СЗИ от НСД в соответствии с действующей нормативной документацией определяет требования на уровне функционала (согласно классу защищённости АС) и не учитывает динамические свойства СЗИ,

что приводит к увеличению времени отклика на запрос пользователя в АС и является неприемлемым для эффективного функционирования этих систем. Согласно пункту 3.6 [11] для устранения указанного недостатка необходимо проводить количественную оценку эффективности СЗИ от НСД для исследования их динамических свойств. Перспективной в этом смысле является предложенная частная методика, базирующаяся на теории математического и эволюционного моделирования, поскольку позволяет получать оптимальные количественные параметры эффективности функционирования СЗИ от НСД [2, 12, 13].

Вывод. Таким образом, в статье предложена частная методика формирования требований к СЗИ от НСД в АС с использованием генетического алгоритма, избавленная от недостатков существующей методики, изложенной в [2]. Разработанная частная методика обладает практической ценностью и позволяет формировать количественные требования к широкому классу сертифицированных по определённому классу защищённости АС в соответствии требованиями действующей нормативной документации.

Библиографический список:

1. Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента Российской Федерации № 646 от 05.12.2016.
2. Методы и средства эволюционного моделирования при обосновании требований к программным системам защиты информации: монография / А.А. Змеев [и др.]; под ред. проф. Е.А. Рогозина. – Воронеж: Воронежский институт МВД России, 2015. – 98 с.
3. Типовая система защиты информации от несанкционированного доступа RU.48957919.501410-0231 // Техническая документация. – Государственный научно-исследовательский институт моделирования интеллектуальных сложных систем, 2017. – 16 с.
4. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удалённого доступа: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (1,62 Мб) / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013. – 265 с.
5. Советов Б.Я. Моделирование систем: учеб. для вузов / Б.Я. Советов, С.А. Яковлев. – 3-е изд., перераб. и доп. – М.: Высш. шк., 2001. – 343 с.
6. Мараховский В.Б. Моделирование параллельных процессов. Сети Петри / В.Б. Мараховский, Л.Я. Розенблюм, А.В. Яковлев. – СПб.: Профессиональная литература, 2014. – 400 с.
7. Ломазова И.А. Вложенные сети Петри: моделирование и анализ распределённых систем с объектной структурой / И.А. Ломазова. – М.: Научный Мир, 2004. – 208 с.
8. Тихонов В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов. – М.: Сов. Радио, 1977. – 488 с.
9. Венцель Е.С. Теория вероятностей / Е.С. Венцель. – М.: Наука, 1969. – 576 с.
10. Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса / И.Г. Дровникова [и др.] // Труды СПИИРАН. № 3 (52) (2017). – С.-Пб.: СПИИРАН, 2017. – 2017. – № 3(52). – С. 234-258. – DOI 10.15622/sp.52.
11. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утв. решением Гостехкомиссии Российской Федерации от 30.03.1992.
12. Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning / D.E. Goldberg. — Massachusetts: Addison-Wesley, 1989.
13. Mitchell M. An Introduction to Genetic Algorithms / M. Mitchell. — Cambridge: MIT Press, 1999. — 158 p.

References:

1. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii. Utv. Ukazom Prezidenta Rossiyskoy Federatsii № 646 ot 05.12.2016. [The information security doctrine of the Russian Federation. Approved by the decree of the President of the Russian Federation No. 646 from 05.12.2016. (In Russ)]
2. Metody i sredstva evolyutsionnogo modelirovaniya pri obosnovanii trebovaniy k programmnym sistemam zashchity informatsii: monografiya / A.A. Zmeyev [i dr.]; pod red. prof. Ye.A. Rogozina. – Voronezh: Voronezhskiy institut MVD Rossii, 2015. – 98 c. [Methods and tools of evolutionary modeling in support of requirements for software systems of information protection: monograph / A.A. Zmeev [and others]; under the editorship of Professor E.A. Rogozin. – Voronezh: Voronezh Institute of MIA Russia, 2015. – 98 p. (In Russ)]
3. Tipovaya sistema zashchity informatsii ot nesanktsionirovannogo dostupa RU.48957919.501410-0231 // Tekhnicheskaya dokumentatsiya. – Gosudarstvennyy nauchno-issledovatel'skiy institut modelirovaniya intellektual'nykh slozhnykh sistem, 2017. – 16 s. [A typical system of information protection from unauthorized access EN.48957919.501410-02 31 // Technical documentation. – State scientific-research Institute of intelligent simulation of complex systems, 2017. – 16 p. (In Russ)]
4. Rad'ko N.M. Proniknoveniya v operatsionnuyu sredu komp'yutera: modeli zloumyshlennogo uda-lonnogo dostupa: ucheb. posobiye [Elektronnyy resurs]. – Elektron. tekstovyye, graf. dannyye (1,62 Mb) / N.M. Rad'ko, YU.K.

YAzov, N.N. Korneyeva. – Voronezh: FGBOU VPO «Voronezhskiy gosudarstvennyy tekhniche-skiy universitet», 2013. – 265 s. [Radko N.M. Penetration into the operating environment of the computer: model malicious remote access: proc. Handbook [Electronic resource]. – Electron. text, count. data (1.62 MB) / N.M. Radko, Yu.K. Yazov, N.N. Korneeva. – Voronezh: FGBOU VPO «Voronezh state technical university», 2013. – 265 p. (In Russ)]

5. . Sovetov B.YA. Modelirovaniye sistem: ucheb. dlya vuzov / B.YA. Sovetov, S.A. Yakovlev. – 3-ye izd., pererab. i dop. – M.: Vyssh. shk., 2001. – 343 s. [Sovetov B.Y. Modelling of systems: proc. for universities / B.Y. Sovetov, S.A. Yakovlev. – 3rd d. rev. and extra. – M.: Higher. wk., 2001. – 343 p. (In Russ)]

6. Marakhovskiy V.B. Modelirovaniye parallel'nykh protsessov. Seti Petri / V.B. Marakhovskiy, L.YA. Rozenblyum, A.V. Yakovlev. – SPb.: Professional'naya literatura, 2014. – 400 s. [Marakhovsky V.B. Modeling of parallel processes. Petri nets / V.B. Marakhovsky, L.Y. Rosenblum, A.V. Yakovlev. – SPb.: Professional literature, 2014. – 400 p. (In Russ)]

7. Lomazova I.A. Vlozhennyye seti Petri: modelirovaniye i analiz raspredelonnykh sistem s ob"-yektnoy strukturoy / I.A. Lomazova. – M.: Nauchnyy Mir, 2004. – 208 s. [Lomazova I.A. Nested Petri nets: modeling and analysis of distributed systems with object structure / I.A. Lomazova. – M.: Scientific World, 2004. – 208 p. (In Russ)]

8. Tikhonov V.I. Markovskiye protsessy / V.I. Tikhonov, M.A. Mironov. – M.: Sov. Radio, 1977. – 488 s. [Tikhonov V.I. Markov processes / V.I. Tikhonov, M.A. Mironov. – M.: Owls. Radio, 1977. – 488 p. (In Russ)]

9. Ventsel' Ye.S. Teoriya veroyatnostey / Ye.S. Ventsel'. – M.: Nauka, 1969. – 576 s. [Ventsel E.S. Probability theory / E.S. Wenzel. – M.: Nauka, 1969. – 576 p. (In Russ)]

10. Matematicheskaya model' otsenki effektivnosti sistem zashchity informatsii s ispol'zovaniyem preobrazovaniya Laplasa i chislennogo metoda Givensa / I.G. Drovnikova [i dr.] // Trudy SPIIRAN. № 3 (52) (2017). – S.-Pb.: SPIIRAN, 2017. – 2017. – № 3(52). – S. 234-258. – DOI 10.15622/sp.52. [Mathematical model of evaluation of the effectiveness of information security systems using the Laplace transform and the numerical method Givens / I.G. Drovnikova [and others] // Proceedings of SPIIRAS. № 3 (52) (2017). – S.-Pb.: SPIIRAS, 2017. – 2017. – № 3(52). – P. 234-258. – DOI 10.15622/sp.52. (In Russ)]

11. Rukovodyashchiy dokument. Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatiziro-vannykh sistem ot nesanktsionirovannogo dostupa k informatsii. Utv. resheniyem Gostekhkomissii Rossiy-skoy Federatsii ot 30.03.1992. [Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information. Approved by the decision of gostekhkomissii of the Russian Federation from 30.03.1992. (In Russ)]

12. Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning / D.E. Goldberg. — Massachusetts: Addison-Wesley, 1989. [Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning / D.E. Goldberg. — Massachusetts: Addison-Wesley, 1989.

13. Mitchell M. An Introduction to Genetic Algorithms / M. Mitchell. — Cambridge: MIT Press, 1999. — 158 p.

Сведения об авторах:

Дровникова Ирина Григорьевна – доктор технических наук, доцент, профессор, кафедра автоматизированных информационных систем органов внутренних дел.

Змеев Анатолий Анатольевич – соискатель кафедры № 12.

Рогозин Евгений Алексеевич – доктор технических наук, профессор, профессор, кафедра автоматизированных информационных систем органов внутренних дел

Information about the authors:

Irina G. Drovnikova – Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Anatoly A. Zmeev - Applicant, Department № 12.

Evgeny A. Rogozin - Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию 07.07.2018.
Принята в печать 10.09.2018.

Conflict of interest.
The authors declare no conflict of interest.

Received 07.07.2018.
Accepted for publication 10.09.2018.