

УДК 004.056
DOI: 10.15827/0236-235X.116.118-124

Дата подачи статьи: 11.10.16
2016. Т. 29. № 4. С. 118–124

ПРОГРАММНАЯ СИСТЕМА СТРУКТУРНО-ПАРАМЕТРИЧЕСКОГО СИНТЕЗА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В.Г. Жуков, к.т.н., доцент, vadimzhukov@mail.ru;

М.Н. Жукова, к.т.н., доцент, mariem@inbox.ru;

А.С. Тимохович, к.п.н., TASStepanich@yandex.ru;

Д.С. Волков, студент, 23_dimon@mail.ru

*(Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева,
просп. им. газ. «Красноярский рабочий», 31, г. Красноярск, 660014, Россия)*

Статья посвящена решению актуальной задачи разработки алгоритма структурно-параметрического синтеза системы защиты информации на примере создания защищенной автоматизированной системы. Данный алгоритм позволяет генерировать несколько возможных вариантов системы защиты информации с учетом требований государственных стандартов в области информационной безопасности, нормативно-методических документов ФСТЭК России и ФСБ России. Кроме этого, каждая сформированная архитектура системы защиты информации предполагает использование достаточно большого количества средств защиты информации, что усложняет задачу из-за появления различных вариантов реализации сформированной архитектуры системы. В работе рассматриваются только сертифицированные средства защиты информации для реализации в рамках построенной архитектуры системы защиты информации. Получившаяся задача оптимизации имеет множество особенностей и ограничений. Классические методы оптимизации в данном случае применить нельзя. Проведен анализ различных схем применения генетического алгоритма оптимизации, хорошо зарекомендовавшего себя при решении подобных задач оптимизации. Однако применение классического генетического алгоритма оказалось невозможным из-за особенностей требований нормативно-методических документов, регуляторов в сфере информационной безопасности, самой структуры системы защиты информации и компонент в виде средств защиты информации. Проведено множество модификаций алгоритма, позволяющих применять разработанный алгоритм при решении реальных практических задач. Разработанный алгоритм с модификациями реализован в виде программного средства. Работа программного средства протестирована при различных вариантах требований к создаваемой системе защиты информации. Эффективность структурно-параметрического синтеза системы защиты информации при использовании разработанного программного средства составляет в среднем 84 %.

Ключевые слова: *структурно-параметрический синтез, система защиты информации, информационная безопасность, проектирование, защищенность, генетический алгоритм.*

По данным аналитического центра InfoWatch, в первом полугодии 2015 года в мире обнародовано (в СМИ и иных источниках) и зарегистрировано 723 случая утечки конфиденциальной информации, что на 10 % превышает количество утечек, зарегистрированных за аналогичный период 2014 года [1]. Внешние атаки стали причиной 32 % утечек данных. В настоящее время в большинстве организаций ведется работа с информацией, требующей защиты в соответствии с нормативно-правовыми актами. А это значит, что необходимо проектировать *систему защиты информации (СЗИ)* так, чтобы избежать утечек [2].

Эта задача ложится на специалиста по информационной безопасности. Ему необходимо проанализировать рынок средств защиты информации и на основе требований создать эффективную систему защиты. При этом надо исходить из того, что основной целью организации является получение прибыли и, следовательно, затраты на систему защиты должны быть экономически оправданы, а сама система не должна создавать трудностей при работе персонала. Все работы по проектированию архитектуры СЗИ специалисту приходится делать практически вручную, затрачивая достаточно много времени. К тому же большую роль играют компетентность и опыт. Чтобы минимизировать

вероятность ошибки проектирования, временные и экономические затраты и помочь специалисту при выборе, необходимо использовать методы автоматизации. В работе рассматривается подход к построению и настройке СЗИ путем использования структурно-параметрического синтеза на базе генетического алгоритма оптимизации.

Проектирование СЗИ

Для обеспечения защиты необходимо использовать средства, которые существенно затруднят для злоумышленника возможность атаки или полностью ее исключат и тем самым снизят риск потери данных в системе. Все средства защиты информации можно разделить на две большие группы: организационные и технические. В любой организации должны быть использованы как те, так и другие средства для создания системы защиты, соответствующей требованиям.

Организационные средства включают в себя организационно-технические и организационно-правовые и являются основой СЗИ, поскольку именно при их помощи определяются порядок и правила функционирования объектов защиты и деятельность должностных лиц по обеспечению защиты информации. Но во многих случаях создание эф-

фактивной СЗИ невозможно без использования технических средств защиты.

Технические средства защиты можно разделить на аппаратные, программные и программно-аппаратные. Основная задача технических средств защиты – блокирование каналов утечки информации для предотвращения утечек, хищения, утрат, искажения, подделки информации.

Согласно Положению ФСТЭК «О сертификации средств защиты информации по требованиям безопасности информации», средства защиты информации, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством, обязательно должны быть сертифицированы. Поэтому для корректной работы разрабатываемого программного средства исходные данные должны быть взяты из реестра сертифицированных на территории России средств защиты информации.

Для качественной защиты информации недостаточно просто установить средства защиты на каждый элемент автоматизированной системы. Необходимо, чтобы все средства, методы и мероприятия, используемые для защиты информации, объединялись в единый целостный механизм – систему защиты.

СЗИ является совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (ГОСТ Р 50922-2006).

При разработке системы защиты чаще всего используется типовый набор технических и организационных средств защиты информации. В статье [3] предлагаются следующие элементы, входящие в типовую схему организации защиты передачи и хранения информации:

- средства защиты от *несанкционированного доступа* (НСД);
- *межсетевой экран* (МЭ);
- средства криптографической защиты информации;
- средства аутентификации и хранения ключевой информации;
- антивирусное ПО;
- *системы обнаружения вторжений* (СОВ);
- средства анализа защищенности;
- операционная система.

Архитектура системы защиты должна соответствовать архитектуре защищаемой системы и быть максимально экономичной, поэтому некоторые из рассмотренных элементов могут отсутствовать в создаваемой системе.

Поскольку количество используемых средств защиты информации очень велико, возникает до-

полнительная сложная задача – правильно описать структуру и параметры системы для эффективного подбора средств и их последующей настройки.

Структурно-параметрический синтез СЗИ

Структурно-параметрический синтез – это процесс, в результате которого определяется структура объекта и находятся значения параметров составляющих ее элементов таким образом, чтобы были удовлетворены условия задания на синтез (технического задания). Так как все объекты и системы на определенном уровне рассмотрения имеют структуру, а элементы, составляющие структуру, имеют параметры, практически любая задача проектирования может быть сведена к задаче структурно-параметрического синтеза [4].

Использование методов структурно-параметрического синтеза для построения архитектуры и настройки параметров СЗИ сопряжено с несколькими проблемами. В работе [5] автор выделяет следующие:

- недостаточные вычислительные мощности;
- отсутствие адекватных языков программирования (в частности, языков, поддерживающих парадигму объектно-ориентированного программирования);
- затруднения в многократном использовании программного кода;
- трудность реализации межплатформенных систем;
- отсутствие общей теории структурно-параметрического синтеза, пригодной для всех классов проектируемых устройств;
- отсутствие совершенного лингвистического обеспечения, поддерживающего процедуру структурно-параметрического синтеза.

Математические и компьютерные модели, применяемые при автоматизации структурно-параметрического синтеза объектов, существенно отличаются от моделей, используемых при автоматизации параметрического синтеза [6]. Так, если при параметрическом синтезе структура объекта в процессе синтеза остается постоянной, то в процессе структурно-параметрического синтеза изменяются как параметры объекта, так и его структура. Сравнение характеристик моделей, применяемых при автоматизации параметрического и структурно-параметрического синтеза, дано в работе [7].

Проектирование системы защиты с использованием алгоритмов синтеза в общем случае можно представить в виде обобщенной схемы, представленной на рисунке 1.

На вход схемы подаются необходимые параметры системы и БД, из которой выбираются средства для проведения синтеза структуры и синтеза параметров. Задача синтеза в данном случае является нетривиальной из-за необходимости учета

требований регуляторов и использования для формирования архитектуры системы защиты довольно большого перечня средств защиты информации. Из-за этих особенностей использование классических методов оптимизации становится сложным или невозможным и необходимо применять другие методы для решения задачи.

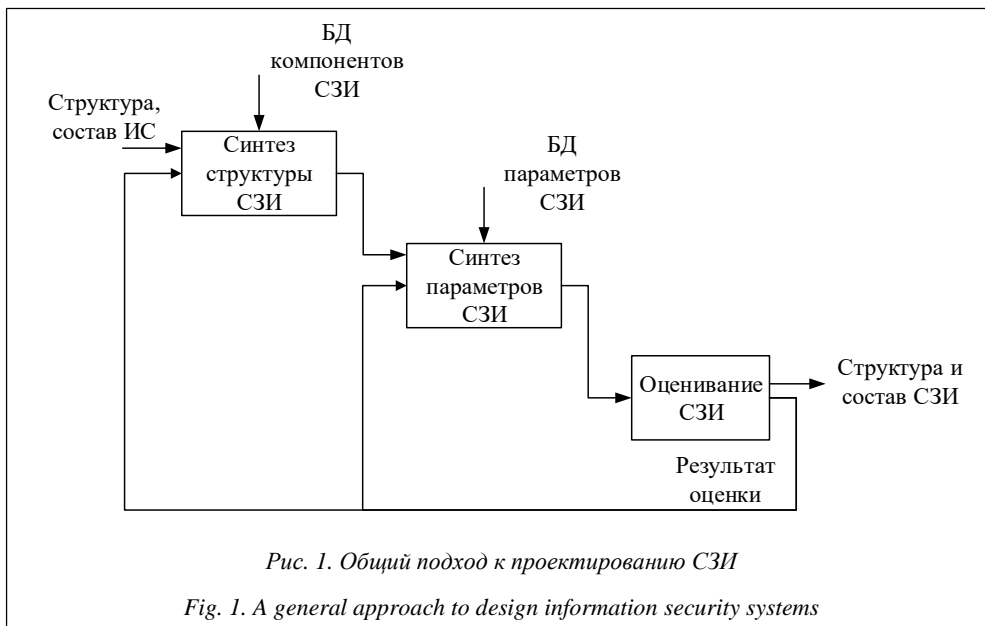


Рис. 1. Общий подход к проектированию СЗИ

Fig. 1. A general approach to design information security systems

Генетический алгоритм оптимизации для решения задачи структурно-параметрического синтеза СЗИ

Требуется решение следующих задач:

- достижение максимума совпадений между заданной пользователем структурой и подобранными средствами защиты;
- достижение максимума совпадений между заданными пользователем параметрами средств защиты и подобранными средствами с этими параметрами;
- минимизация стоимости решения.

Таким образом, формируется следующая задача оптимизации:

$$F(X) = \begin{cases} 0, x_i \neq x_i^* \\ 1, x_i = x_i^* \end{cases} \rightarrow \max, \quad (1)$$

где $X = (x_1, \dots, x_n)$ при $n = 53$, $x \in [a_i; b_i]$, $C \leq C^*$ (стоимость), $C \rightarrow \min$.

Исходя из выбранной типовой структуры и параметров средств защиты, пользователь может задать 256 различных сочетаний элементов структур и 211 680 сочетаний различных параметров данных средств защиты.

Реестр сертифицированных средств в ФСТЭК содержит 1 226 записей, из которых элементами выбранной структуры являются следующие:

- средства защиты от НСД – 32 записи;
- МЭ – 387 записей;
- средства аутентификации и хранения ключевой информации – 15 записей;
- антивирусное ПО – 16 записей;
- СОВ – 14 записей;
- средства анализа защищенности – 4 записи;
- операционные системы – 64 записи.

Каждое из данных средств имеет набор параметров и стоимость. Для решения задачи предлагается использовать генетические алгоритмы.

Генетический алгоритм (англ. genetic algorithm) – это эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путем случайного подбора, комбинирования и вариации искоемых параметров с использованием механизмов, аналогичных естественному отбору в природе [8]. Первые работы по применению генетических алгоритмов были проведены в 1954 году, а особенно популярными они стали благодаря работе Джона Холланда и его книге «Адаптация в естественных и искусственных системах» в начале 70-х годов.

В статье [9] Холланд описывает типовую схему работы генетического алгоритма:

- а) задание целевой функции (приспособленности) для особой популяции;
- б) создание начальной популяции;
- в) отбор особей для скрещивания;
- г) подбор пар для скрещивания;
- д) скрещивание;
- е) мутирование;
- ж) вычисление значений целевой функции для каждой особи;
- и) формирование нового поколения (селекция);
- к) если выполняются условия остановки, цикл заканчивается, иначе – возвращаемся к шагу в).

В работе проведен анализ различных схем работы операторов. С учетом особенностей поставленной задачи сделан следующий выбор:

- схема отбора особей – пропорциональный отбор; данная схема наиболее просто реализуется и не требует дополнительных затрат вычислительной мощности на сортировку массива, необходимую в других способах;

- схема подбора особей в родительскую пару – случайный способ выбора; поскольку эта схема является универсальной для решения различных классов задач и численность популяции в рассматриваемой задаче достаточно мала;
- схема скрещивания – одноточечный кроссинговер;
- схема формирования нового поколения – в следующее поколение переходят и родители, и потомки без использования принципа элитизма;
- схема мутации – точечная мутация.

Программная система структурно-параметрического синтеза СЗИ

Для проведения структурно-параметрического синтеза СЗИ разработано программное средство, обобщенная схема которого показана на рисунке 2. На рисунке 3 приведена блок-схема работы программного средства.

Перед началом работы пользователь задает необходимые параметры системы при помощи элементов формы главного окна программы (см. <http://www.swsys.ru/uploaded/image/2016-4/2016-4-dop/3.jpg>). Пользователь системы может лишь выбрать необходимый класс защищенности автоматизированной системы и (или) класс персональных данных и получить автоматически сформированный список требований по структуре и параметрам системы, который будет подан на вход алгоритма для дальнейшего подбора подходящих средств защиты, либо самостоятельно осуществить выбор средств защиты информации в соответствии с существующими потребностями организации или требованиями регулирующими органов.

После нажатия на кнопку «Старт» происходит обработка введенной информации и генерация целевой функции, максимума которой необходимо достичь. Значением данной функции является количество бит, стоящих на гене на тех же местах, что и в значении, которое ввел пользователь. После этого происходит считывание информации о средствах защиты информации из текстового файла формата .txt, получаемого путем экспорта его из таблицы Excel. Каждый элемент в базе имеет следующий набор параметров:

- название;
- класс средств защиты из перечня типовых средств (8 бит);
- класс защищенности средств вычислительной техники (СВТ) от НСД (7 бит);

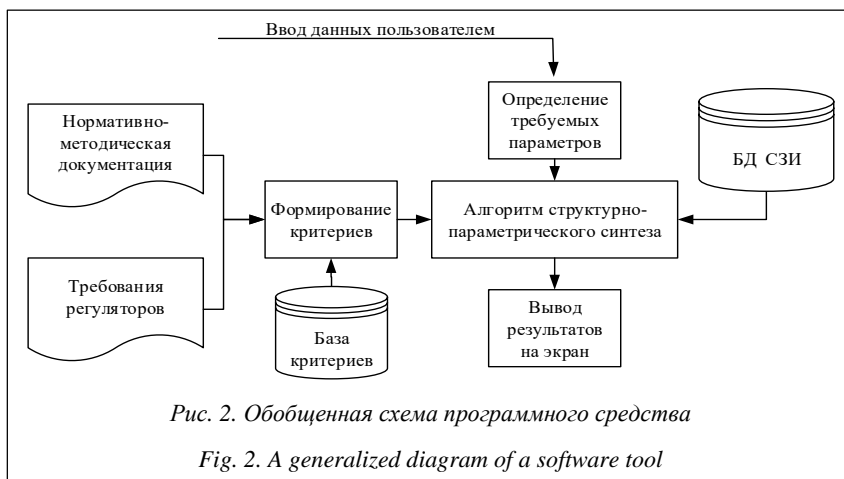


Рис. 2. Обобщенная схема программного средства

Fig. 2. A generalized diagram of a software tool

- класс защиты по недеklarированным возможностям (НДВ) (4 бита);
- класс МЭ (5 бит);
- оценочный уровень доверия (ОУД) (7 бит);
- класс СОВ (6 бит);
- класс средств антивирусной защиты (САВЗ) (6 бит);
- класс ФСБ (6 бит);
- стоимость.

На рисунке 4 показан порядок расположения бит в БД.

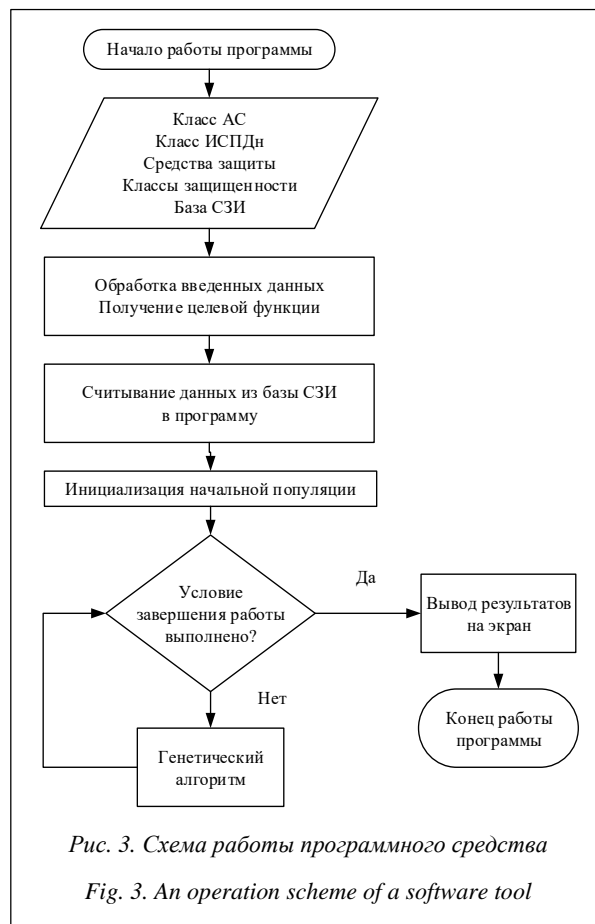


Рис. 3. Схема работы программного средства

Fig. 3. An operation scheme of a software tool

Название	СЗИ								СВТ от НСД							НДВ				МЭ					Цена
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	1	2	3	4	1	2	3	4	5	
	ОУД								СОВ							САВЗ				ФСБ					
	1	2	3	4	5	6	7	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6

Рис. 4. Расположение бит в базе СЗИ

Fig. 4. The arrangement of bytes in an information security system base

Континет 3.7	СЗИ								СВТ от НСД							НДВ				МЭ					111 550		
	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1		1	1
	ОУД								СОВ							САВЗ				ФСБ							
	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0		

Рис. 5. Пример записи БД

Fig. 5. An example of a database record

Пример записи, имеющейся в БД, показан на рисунке 5.

Данное средство защиты имеет сертификаты ФСТЭК по 2-му уровню контроля НДВ, 2-му классу МЭ, 3-му классу СОВ и сертификат ФСБ по классу комплекса средств защиты (КСЗ).

После считывания БД и занесения ее в структуру происходит инициализация начальной популяции. Для этого каждый элемент из БД сравнивается со значением, которого необходимо достичь, и вся популяция сортируется. Затем из нее выбираются лучшие особи.

На следующем шаге происходит проверка условия завершения работы. Работа завершается, если найдено решение, удовлетворяющее заданным параметрам, или превышено максимальное число поколений. Второе условие необходимо, чтобы исключить возможность заикливания алгоритма в ситуациях, когда невозможно найти решение.

Для вычисления приспособленности каждой особи необходимо взять отношение среднего значения целевой функции в популяции к значению функции особи, для которой производится расчет. Приспособленность необходима для дальнейшего использования схемы пропорционального отбора.

Далее формируем промежуточное поколение, которое и будет результатом отбора особей. Все отобранные особи случайным образом разбиваются на пары, и производится скрещивание. При этом необходимо учитывать ряд особенностей, которые возникают в зависимости от поставленной задачи и способа реализации. Можно выделить следующие особенности реализации генетического алгоритма в программной системе:

- в программе для хранения характеристик используется тип `unsigned __int64`, вследствие этого для выполнения скрещивания необходимо использовать операции побитового сдвига влево и вправо;
- необходимость в каждом гене хранить информацию о том, результатом скрещивания каких особей он является, чтобы в конце работы алгоритма по подобранному решению можно было выявить, из каких средств защиты оно состоит.

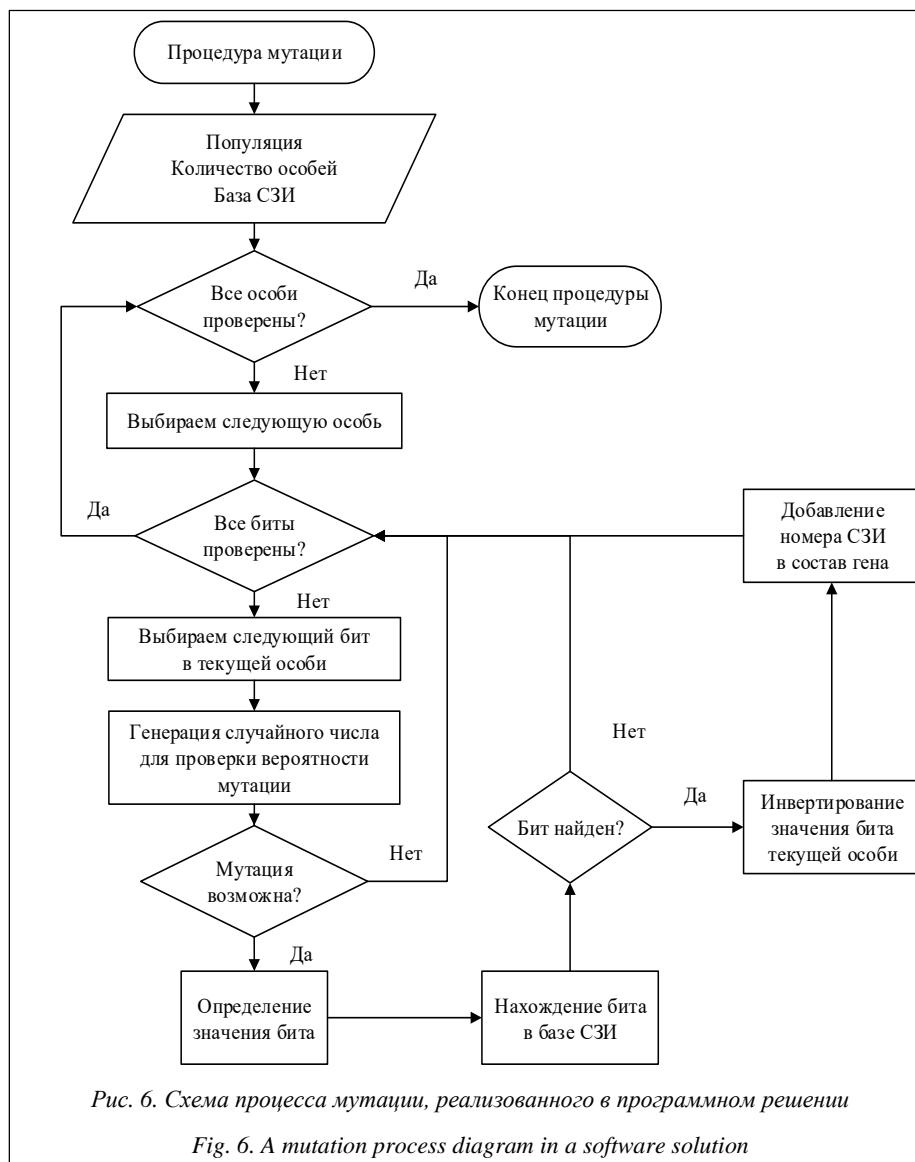
После проведения скрещивания выполняется процедура мутации для всех особей в промежуточной популяции. Для поставленной задачи при каждой мутации необходимо проверить ее возможность. Мутация возможна только в случае, если соответствующий бит имеется в БД. Процедура мутации осуществляется следующим образом:

- по порядку выбирается каждый бит в каждой особи;
- генерируется случайное дробное число в диапазоне от 0 до 1;
- сравниваются полученное число и вероятность мутации, заданная параметром работы алгоритма;
- если мутация оказалась возможной, определяется значение бита, стоящего на данной позиции, и проверяется его наличие в БД, иначе мутация не происходит и выбирается следующий бит;
- если в БД одно и более средств имеют данный бит, случайным образом выбирается одно из них, иначе мутация не происходит и выбирается следующий бит;
- значение бита меняется на противоположное в данной позиции;
- номер средства защиты, в котором был найден данный бит, вносится в состав гена.

Блок-схема данного процесса представлена на рисунке 6.

После мутации производится пересчет значений путем сравнения особей со значением, которое ввел пользователь, и отбор лучших из них. Далее происходит проверка завершения работы алгоритма и вывод решения на экран в виде списка необходимых средств защиты (см. <http://www.swsys.ru/uploaded/image/2016-4/2016-4-dop/4.jpg>).

Задача синтеза СЗИ является сложной из-за одновременного учета требований со стороны нормативно-методических требований и требований регуляторов в сфере информационной безопасности, а также огромного количества решений, возможных при применении тех или иных стратегий разработки СЗИ. Кроме этого, каждая сформирован-



ментов, регуляторов в сфере информационной безопасности, самой структуры СЗИ и компонент в виде СЗИ. Проведено множество модификаций алгоритма, позволяющих применять разработанный алгоритм при решении реальных практических задач.

Разработанный алгоритм с модификациями реализован в виде программного средства, позволяющего универсально применять его для проектирования и настройки СЗИ для организаций различной формы собственности (государственные учреждения, коммерческие компании), а также различных масштабов. Работа программного средства протестирована с учетом различных вариантов требований к создаваемой СЗИ. Эффективность структурно-параметрического синтеза СЗИ при использовании разработанного программного средства составляет в среднем 84 %.

ная архитектура СЗИ предполагает использование достаточно большого количества средств защиты информации, что усложняет задачу из-за появления различных вариантов реализации сформированной архитектуры СЗИ. В работе (из-за универсальности разрабатываемого решения – для применения в государственных или коммерческих организациях) принято решение рассматривать только сертифицированные средства защиты информации для реализации в рамках построенной архитектуры СЗИ. Получившаяся задача оптимизации имеет множество особенностей и ограничений. Классические методы оптимизации в данном случае оказались неприменимыми. Проведен анализ различных схем применения генетического алгоритма оптимизации, хорошо зарекомендовавшего себя при решении подобных задач оптимизации. Однако применение классического генетического алгоритма оказалось невозможным из-за особенностей требований нормативно-методических доку-

Литература

1. InfoWatch: Исследование утечек информации за первое полугодие 2015 года. URL: <http://www.infowatch.ru/analytics/reports/16340> (дата обращения: 30.03.2016).
2. Zhukova M., Stefarov A. Development of the protected telecommunication systems. Proc. 2015 Intern. Siberian Conf. on Control and Communications (SIBCON 2015). URL: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84941051058&partnerID=40&md5=ad5536b24acf44c96921ec62626aa70f> (дата обращения: 30.03.2016).
3. InformationSecurity: Типовая схема организации защиты передачи и хранения информации. URL: http://www.itsec.ru/articles2/Inf_security/tipovaya-shema-organizacii-zaschiti-pere-dachi-i-hraneniya-informacii (дата обращения: 09.04.2016).
4. Жукова М.Н. О структурно-параметрическом синтезе защищенных информационных систем // Решетневские чтения: матер. XIX Междунар. науч. конф. Красноярск: Изд-во СибГАУ, 2015. Ч. 2. С. 282–284.
5. Акимов С.В. Анализ проблемы автоматизации структурно-параметрического синтеза // Доклады ТУСУР. 2011. № 2 (24). С. 204–211.
6. Бухтояров В.В., Жуков В.Г., Жукова М.Н., Золота-

рев В.В., Ковалев И.В., Попов А.М. Поддержка принятия решений при проектировании систем защиты информации: монография. М.: ИНФРА-М, 2014. 131 с.

7. Акимов С.В. Компьютерные модели для автоматизированного структурно-параметрического синтеза // Компьютерное моделирование 2004: тр. 5-й Междунар. конф. СПб: Нестор,

2004. Ч. 1. С. 191–197.

8. CodeNet: Что такое генетический алгоритм? URL: <http://www.codenet.ru/progr/alg/Smart/Genetic-Algorithms.php> (дата обращения: 31.03.2016).

9. Джон Х. Холланд. Генетические алгоритмы // В мире науки. 1992. № 9–10. С. 32–40.

Software & Systems

DOI: 10.15827/0236-235X.116.118-124

Received 11.10.16

2016, vol. 29, no. 4, pp. 118–124

PROGRAM SYSTEM OF STRUCTURAL AND PARAMETRICAL SYNTHESIS OF AN INFORMATION SECURITY SYSTEM

V.G. Zhukov¹, Ph.D. (Engineering), Associate Professor, vadimzhukov@mail.ru

M.N. Zhukova¹, Ph.D. (Engineering), Associate Professor, mariem@inbox.ru

A.S. Timokhovich¹, Ph.D. (Education), TASstepanich@yandex.ru

D.S. Volkov¹, Student, 23_dimon@mail.ru

¹Academician M.F. Reshetnev Siberian State Aerospace University, Krasnoyarsky Rabochy Ave. 31, Krasnoyarsk, 660014, Russian Federation

Abstract. The article is devoted to the solution of an important problem of structural and parametrical synthesis algorithm development for an information security system on the example of creating a protected automated system. This algorithm allows generating several possible options of an information security system considering requirements of state standards in the field of information security, standard and methodical documents of the Federal Service for Technical and Export Control of Russia and the Federal Security Service of Russia. Besides, each architecture of an information security system assumes using rather large number of information security means. It complicates the task because of various options of information security system created architecture implementation. The paper considers only certified means of information security for implementation within the constructed architecture of information security system. Such problem of optimization has a set of features and restrictions. Classical optimization methods in this case aren't applicable. The analysis of various schemes of application of an optimization genetic algorithm which has proved itself when solving similar problems of optimization. However, application of a classical genetic algorithm is impossible because of features of requirements of standard and methodical documents, regulators in the information security area, structures of information security system and a component in the form of information protection means. A set of algorithm modifications is carried out. They allow applying the developed algorithm when solving real practical tasks. The developed algorithm with modifications is implemented as software. Software operation is tested at various versions of requirements to the created information security system. The efficiency of structural and parametrical synthesis of an information security system when using the developed software is 84 % at average.

Keywords: structural and parametrical synthesis, information security system, information security, design, security, genetic algorithm.

References

1. *InfoWatch: Issledovanie utechek informatsii za pervoe polugodie 2015 goda* [InfoWatch. Research of information leakages for the first half of 2015]. Available at: <http://www.infowatch.ru/analytics/reports/16340> (accessed March 30, 2016).
2. Zhukova M., Stefarov A. Development of the protected telecommunication systems. Int. *Siberian Conf. on Control and Communications, SIBCON 2015*. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84941051058&partnerID=40&md5=ad5536b24acf44c96921ec62626aa70f> (accessed March 30, 2016).
3. *InformationSecurity: Tipovaya skhema organizatsii zashchity peredachi i khraneniya informatsii* [InformationSecurity. Standard scheme of information transfer and storage protection]. Available at: http://www.itsec.ru/articles2/Inf_security/tipovaya-shema-organizacii-zaschiti-peredachi-i-hraneniya-informacii (accessed March 30, 2016).
4. Zhukova M.N. On structural and parametrical synthesis of secured information systems. *Materialy XIX Mezhdunar. nauch. konf. "Reshetnevskie chteniya"* [Proc. 19th Int. Scientific Conf. Reshetnev's Readings]. Part 2. Krasnoyarsk, SibGAU Publ., 2015, pp. 282–284 (in Russ.).
5. Akimov S.V. The analysis of an structure and parametric synthesis automation problem. *Doklady TUSUR* [Proc. of TUSUR Univ.]. 2011, no. 2 (24), pp. 204–211 (in Russ.).
6. Bukhtoyarov V.V., Zhukov V.G., Zhukova M.N., Zolotarev V.V., Kovalev I.V., Popov A.M. *Podderzhka prinyatiya resheny pri proektirovanii sistem zashchity informatsii* [Decision-making support when designing information security systems]. Moscow, INFRA-M Publ., 2014, pp. 131 (in Russ.).
7. Akimov S.V. Computer models for an automated structural and parametrical synthesis. *Kompyuternoe modelirovanie 2004: Tr. 5 Mezhdunar. konf.* [Proc. 5th Int. Conf. on Computer Modeling 2004]. Part 1, St. Petersburg, Nestor Publ., 2004, pp. 191–197 (in Russ.).
8. *CodeNet: Chto takoe geneticheskyy algoritm?* [CodeNet: What is a genetic algorithm?]. Available at: <http://www.codenet.ru/progr/alg/Smart/Genetic-Algorithms.php> (accessed March 30, 2016).
9. Holland D.K. Genetic Algorithms. *V mire nauki* [In the world of Science]. 1992, no. 9–10, pp. 32–40 (in Russ.).