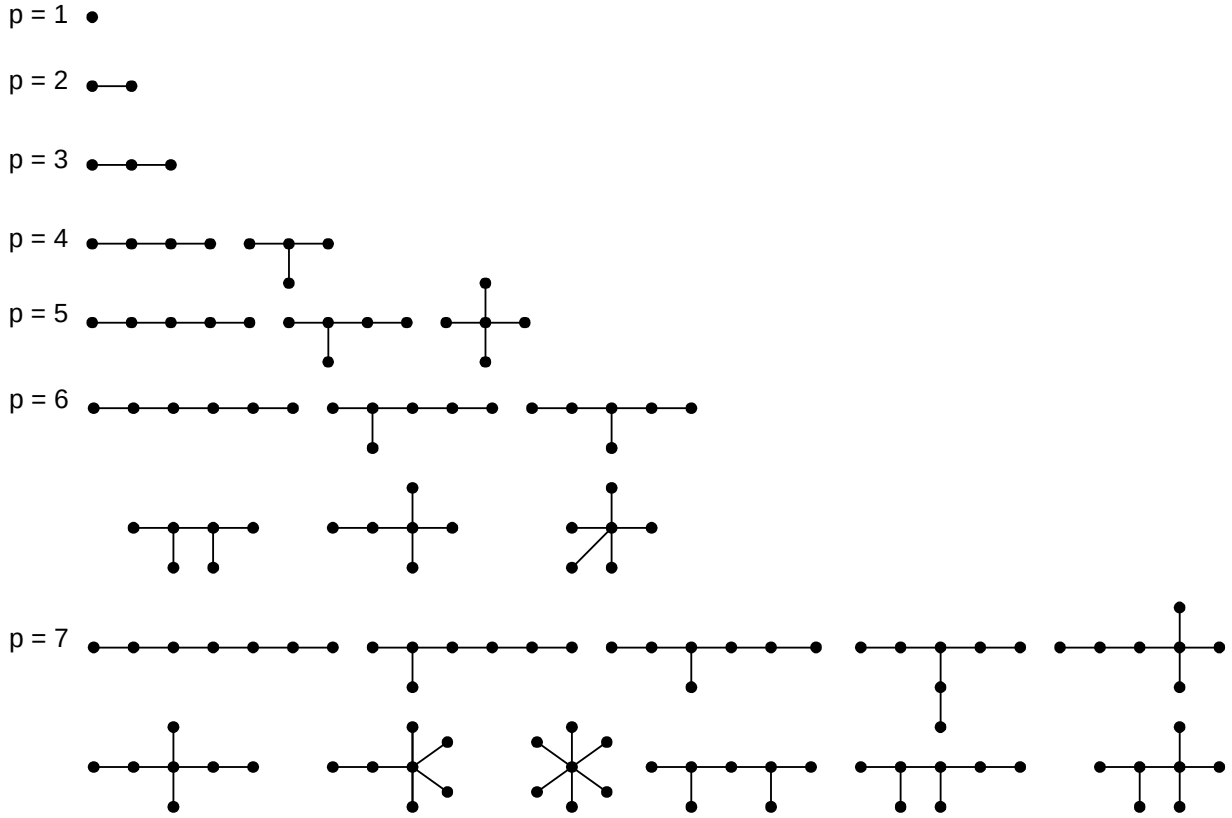
Приложение 1



SHUT V.N. Generation of trees

In clause the technique of calculation of number of the graphic objects having given properties is considered. Such class of tasks is determined in the theory grafov as transfer gravof. The effective algorithm of transfer grafov of a type a tree is developed.

УДК 681.324

Брюхомицкий Ю.А., Казарин М.Н.

МНОГОФАКТОРНАЯ СИСТЕМА ПАРОЛЬНО-КЛАВИАТУРНОЙ АУТЕНТИФИКАЦИИ

Персонализация (идентификация) и подтверждение подлинности (аутентификация) субъектов являются одним из основополагающих принципов обеспечения безопасности функционирования автоматизированных информационных систем (АИС).

Процедура идентификации/аутентификации основана на предъявлении субъектом, по крайней мере, одной из трех сущностей:

- нечто, что он знает;
- нечто, чем он владеет;
- нечто, что есть часть его самого.

Первый принцип реализуется в *парольных системах* идентификации/ аутентификации. Эти системы наиболее просты, при условии правильной организации подбора и использования паролей, являются достаточно надежными и потому широко распространены. Основной недостаток парольных систем заключается в принципиальной оторванности аутентификатора от субъекта-носителя. В результате пароль может быть позаимствован тем или иным способом у законного владельца и использован злоумышленником.

Второй принцип реализуется в интеллектуальных замково-ключевых устройствах, которые образовали класс *персональных средств идентификации*. В них, по существу, совмещаются два тапа идентификатора: парольного и персонального, поэтому их называют еще двухфакторными. Представителями персональных идентификаторов являются токены различных типов и смарт-карты. Двухфакторные средства аутентификации исключают возможность подобрать, подсмотреть или перехватить пароль для входа в АИС, однако персональный идентификатор может быть просто утрачен.

Третьему принципу отвечают только *биометрические параметры организма человека*. При этом для идентификации используются статические параметры: геометрия лица и кистей рук, дактилоскопические узоры пальцев, ладоней и других областей кожи, рисунки радужной оболочка глаза и глазного дна, термограммы артерий и вен, а также динамические параметры: тембр голоса, рукописный и клавиатурный почерки.

Биометрические системы аутентификации имеют ряд неоспоримых преимуществ: биометрические признаки очень трудно фальсифицировать; уникальность биометрических признаков обеспечивает очень высокую достоверность аутентификации; биометрический аутентификатор всегда совмещен с его носителем. Вместе с тем, использование в биометрических системах высоких технологий обуславливают их сравнительно высокую стоимость. Преимущественно это касается систем, использующих статические признаки. Кроме

Брюхомицкий Юрий Анатольевич, *кандидат технических наук, старший научный сотрудник, доцент кафедры безопасности информационных технологий Таганрогского технологического университета Южного федерального университета.*

Казарин Максим Николаевич, *кандидат технических наук, доцент кафедры безопасности информационных технологий Таганрогского технологического университета Южного федерального университета.*

Россия, ТТИ ЮФУ, 347928, г. Таганрог, ул. Чехова, 2.

того, статические биометрические признаки открыты, что создает потенциальную возможность их фальсификации.

Биометрические системы аутентификации на основе динамических признаков существенно дешевле. Это обусловлено тем, что они могут быть реализованы или исключительно программными средствами, или – с использованием стандартных средств мультимедиа (графического планшета, звуковой карты). Достоинством динамической биометрии является также возможность сохранения образа личности в тайне и быстрой его смены за счет смены воспроизводимой контрольной фразы. Недостатком этих систем считается их сравнительно невысокая точность, которая обусловлена зависимостью результата аутентификации от психофизического и психофизиологического состояния человека.

В классе динамической биометрии особое место занимают клавиатурные системы аутентификации (КСА), которые могут удачно сочетать в себе большую часть преимуществ, как статических, так и динамических биометрических систем.

КСА могут быть двух типов:

- для аутентификации пользователя, претендующего на доступ к АИС;
- для проведения скрытного клавиатурного мониторинга пользователей АИС.

В КСА первого типа претендент на доступ производит набор на клавиатуре некоторой контрольной фразы. В процессе набора контрольной фразы КСА производит измерение параметров клавиатурного набора, сравнивает их с эталоном, зарегистрированным для данного пользователя, и по результату сравнения принимает аутентификационное решение.

КСА второго типа позволяют скрытно и непрерывно аутентифицировать пользователя АИС, уже осуществившего легальный вход АИС. Принятие аутентификационного решения в них производится на основе контроля произвольных манипуляций на клавиатуре, произведенных пользователем в течение определенного промежутка времени (т.н. текстонезависимая аутентификация).

В данной работе рассматривается реализация КСА первого типа. Функционирование таких КСА состоит из двух этапов. На первом этапе (этапе регистрации) для каждого регистрируемого в АИС пользователя на основе многократного ввода им фиксированной контрольной фразы формируется биометрический эталон. На втором этапе (идентификации-аутентификации) КСА по предъявленному имени пользователя извлекает из хранилища эталонов биометрический эталон данного пользователя (стадия идентификации). Пользователь вводит на клавиатуре контрольную фразу, при этом текущие параметры ввода сравниваются с биометрическим эталоном данного пользователя. По результатам сравнения принимается аутентификационное решение. Сравнение выполняется на основе использования какой-либо меры близости, обучаемой нейронной сети, параметрических и других методов классификации.

В качестве параметров клавиатурного набора в КСА обычно используются время удержания клавиш и время пауз между удержаниями. Задание в биометрическом эталоне пользователя интервалов допустимых значений измеряемых параметров может осуществляться двумя способами. На малых обучающих выборках целесообразно прямое вычисление минимума и максимума измеренных значений *N* контролируемых параметров: $[\min(v_j), \max(v_j)]$, $j = \overline{1,N}$ [1]. При объеме обучающей выборки в 5 и более примеров становится целесообразным вычисление математического ожидания значений параметров $m(v_j)$ и их дисперсии $\sigma(v_j)$. В этом случае значение минимальной и максимальной границ вычисляют следующим образом [2]:

$$\min(v_j) = m(v_j) - t(L,(1-P_1)) \cdot \sigma(v_j);$$

$$\max(v_j) = m(v_j) + t(L,(1-P_1)) \cdot \sigma(v_j),$$

где L – число использованных при обучении примеров;

P_1 – заданное значение вероятности ошибок первого рода;

$t(L,(1-P_1))$ – коэффициенты Стьюдента.

В конечном итоге совокупность контролируемых биометрических параметров пользователя в процессе его регистрации представляется в виде некоторого эталонного биометрического вектора $\mathbf{V}_Э = (v_1, v_2, ..., v_N)$.

В [3] предложен другой способ представления биометрического эталона пользователя, который основан на конструировании специальной временной функции процесса клавиатурного набора с последующим переводом ее в частотную область. Частотное представление функции реализуется с помощью одного из ортогональных разложений. Коэффициенты разложения являются компонентами эталонного биометрического вектора $\mathbf{V}_Э = (v_1, v_2, ..., v_N)$. На этапе аутентификации вектор биометрических параметров $\mathbf{V}$ претендента на доступ сравнивается с эталонным вектором $\mathbf{V}_Э$, зарегистрированным в КСА на имя данного пользователя. По результатам сравнения принимается аутентификационное решение.

КСА при условии использования открытых контрольных фраз позволяют достичь значений ошибок первого и второго рода порядка 10^{-2} [3, 4]. По сравнению с другими биометрическими системами аутентификации личности, основанными, например, на анализе папиллярных рисунков пальцев рук, имеющими ошибки первого рода 10^{-3} и второго рода 10^{-9}, КСА представляются мало привлекательными. Вместе с тем, практика показывает, что в большинстве АИС массового применения ошибки первого рода на уровне 10^{-2} в большинстве случаев оказывается вполне приемлемыми. Действительно, такая ошибка первого рода соответствует лишь одному случаю отказа легальному пользователю из 100, который быстро преодолевается повторными 1-2 попытками. Другое дело ошибки второго рода, которые собственно и определяют уровень защиты АИС от злоумышленников, предоставляемый подсистемой аутентификации. Уровень 10^{-2} этих ошибок в АИС совершенно не приемлем.

С целью повышения уровня защищенности АИС, использующих КСА, открытую контрольную фразу предлагается заменить секретной (пароль, парольная фраза). При совмещении в одной системе аутентификации процедур парольной и скрытной клавиатурной аутентификации, общий уровень защиты системы (ошибка второго рода) будет определяться одновременно тремя факторами:

- способностью КСА отличить «своего» и «чужого» исключительно по особенностям их биометрии, т.е. при вводе ими одной и той же открытой контрольной фразы;
- «секретностью» вводимой контрольной фразы;
- «секретностью» самого факта наличия биометрического контроля.

В результате образуется трехфакторная парольно-клавиатурная система аутентификации (ПКСА). Первые два фактора определяют уровень защиты в условиях, когда злоумышленник знает о наличии встроенного клавиатурного контроля. Для осуществления несанкционированного доступа в этих условиях злоумышленнику необходимо организовать и совместить две трудоемкие процедуры: подбора пароля и соблюдения определенных клавиатурных особенностей его ввода.

Приведенные в работе [5] результаты исследований показывают, что в биометрической системе аутентификации с рукописным вводом ошибка второго рода при переходе от открытого контрольного слова из 5 букв к секретному слову той же длины уменьшается, в зависимости от стабильности рукописного почерка, на 3-23 десятичных порядка. Для большинства пользователей (38% пользователей, обладающих средней стабильностью рукописного почерка) ошибка второго рода с переходом от открытого слова к секретному слову той же длины уменьшается с 10^{-2} до 10^{-9}, т.е. на 7 десятичных порядков.

Аналогичной статистики для ПКСА пока нет, но есть основания ожидать, что степень снижения ошибки второго рода при переходе от открытой контрольной фразы к паролю в ПКСА будет близка к выше приведенным данным. Это следует из того, что возможные процедуры подбора пароля в обоих случаях одинаковы. Отличия возможны лишь в статистических шкалах уровней стабильности рукописного и клавиатурного почерков. Кроме того, следует принимать во внимание, что длина пароля в ПКСА может быть существенно больше 5 символов, что также дополнительно и существенно увеличит уровень предоставляемой защиты.

Третий фактор («секретность» самого факта наличия биометрического контроля) реализуется путем совмещения процедур парольной и клавиатурной аутентификации на одном штатном интерфейсе аутентификации пользователя используемой ОС. Злоумышленник при попытке НСД видит перед собой стандартное окно парольной аутентификации и не подозревает о наличии дополнительного кла-

виатурного контроля. Поэтому он будет безуспешно пытаться подбирать пароль известными способами, не обращая внимания на особенности его клавиатурного ввода. Третий фактор дополнительно понижает вероятность несанкционированного доступа (ошибку второго рода), достигнутую в двухфакторной системе еще на несколько десятичных порядков.

Таким образом, есть основания полагать, что использование трехфакторной ПКСА вместо однофакторной КСА в значительной мере снижает вероятность несанкционированного доступа в АИС и, соответственно, повышает уровень предоставляемой защиты. При ориентации на компьютерные системы широкого применения важно еще и то, что ПКСА не требует использования никаких дополнительных аппаратных средств. Поэтому общая стоимость реализации предлагаемого подхода по отношению к использованию обычной парольной аутентификации возрастает весьма незначительно, – только за счет стоимости дополнительного программного обеспечения, реализующего ПКСА. Для сравнения, например, стоимость биометрической системы аутентификации по радужной оболочки глаза составляет $500 и выше, по сетчатке глаза – около $4000, причем большую часть цены составляет стоимость специальных аппаратных средств. Возможность чисто программной реализации ПКСА помимо экономии в стоимости, обеспечивает в определенной степени и фактор скрытности биометрического контроля, за счет отсутствия открытых для обозрения специальных аппаратных средств.

Дорогие биометрические системы, удовлетворяющие высоким требованиям по безопасности, применяются, как правило, для контроля доступа к государственной или коммерческой информации, имеющую высокую степень конфиденциальности, т.е. тогда, когда стоимость информации существенно превышает стоимость средств защиты этой информации. Для большого числа коммерческих организаций, фирм, малых офисов, домашних и мобильных компьютеров, где уровень конфиденциальности информации сравнительно невелик, нет смысла в использовании дорогостоящих биометрических систем. Там более желательны надежные системы массового применения (ориентированные на большое число потребителей, обладающие невысокой стоимостью, простотой использования и обслуживания). К таким системам, прежде всего, относятся персональные и мобильные компьютеры (ПК и МК), на которые и ориентирован предлагаемый подход. В ПК, МК по сравнению с мощными многопользовательскими АИС существенно проще и дешевле реализовать дополнительный клавиатурный биометрический контроль доступа на базе существующей в них стандартной процедуры парольной аутентификации. Реализованная в ПК, МК трехфакторная ПКСА становится, по существу, естественным прозрачным расширением стандартной парольной аутентификации. При использовании ПКСА пользователю необходимо лишь знать парольную фразу и научиться ее правильно (однотипно) набирать на клавиатуре компьютера. Стоимость реализации такого решения существенно меньше стоимости биометрических систем на основе статических признаков, обладающих соизмеримыми и даже большими уровнями ошибок аутентификации.

В персональных компьютерах в настоящее время наибольшее распространение получили операционные системы корпорации Microsoft. Поэтому идеи построения трехфакторной ПКСА, в первую очередь, были опробованы в ОС Windows 2000/2003/XP [6].

Как известно, штатная процедура парольной аутентификации пользователя в ОС Windows 2000/2003/XP, основана на использовании хэш-функции LM и NT, причем LM-хэш обладает рядом недостатков и используется в системе для обратной совместимости с более ранними версиями Windows [7]. В худшем случае, используя подбор паролей в «лоб» для LM-хэш (количество возможных символов равно 197) при длине пароля 14 символов, количество возможных вариантов пароля составляет $1{,}33 \cdot 10^{32}$. С учетом того, что «средний» по производительности компьютер способен подбирать пароли со скоростью порядка $1{,}9 \cdot 10^6$ единиц в секунду, для полного перебора потребуется $2{,}2 \cdot 10^9$ млрд. лет. Правда, указанная цифра является сильно завышенной. Исходя из особенностей работы хэш-функции LM, пароль разбивается на две 7-символьные части, каждая из которых кодируется независимо и поэтому для перебора всех возможных комбинаций потребуется (всего!) 197 лет. Такой уровень защиты, предоставляемый штатной парольной аутентификацией в ОС Windows 2000/2003/XP, предлагается существенно увеличить путем дополнения ее скрытной КСА.

Разработка опытного образца программного обеспечения (ПО) ПКСА было основано на методах, описанных в работах [3, 4]. При разработке ПО были поставлены и решены следующие задачи:

- свести к минимуму влияние психофизического и психофизиологического состояния пользователя на результат аутентификации;
- упростить процедуру создания биометрического эталона пользователя (обычно пользователю приходится вводить свой пароль не менее 20 раз);
- усилить способность биометрической системы анализировать слабо выраженный клавиатурный почерк «среднего» пользователя;
- заложить возможность автоматического изменения биометрического эталона пользователя по мере накопления устойчивых изменений в динамике его работы на клавиатуре.

Результатом разработки стал программный продукт BioKeyProtect, который позволят дополнить стандартную парольную процедуру входа в ОС скрытной КСА. Данный программный продукт работает с ОС Windows 2000/2003/XP и ориентирован на использование в домашних условиях, небольших фирмах и организациях.

BioKeyProtect полностью интегрируется в ОС и работает прозрачно для пользователя. Пользователь, так же как и раньше (до внедрения ПКСА), пользуясь стандартным диалоговым окном парольной аутентификации Windows 2000/2003/XP, осуществляет вход в систему по паролю, но при этом прозрачно для него происходит проверка правильности динамики клавиатурного ввода пароля. В случае если динамика клавиатурного ввода пароля отличается от эталонного значения для данного пользователя, система реагирует точно так же, как при вводе ошибочного пароля. Поэтому, если злоумышленник, владеющий верным паролем, будет делать попытки входа в систему с установленной защитой BioKeyProtect, то с очень большой вероятностью он получит отказ. Причем система будет настойчиво выдавать сообщение об ошибочности самого пароля.

Процедура скрытной биометрической аутентификации по клавиатурному почерку включается после прохождения штатной идентификации по имени и только для тех пользователей, для которых в системе хранится биометрический эталон. Для аутентификации остальных пользователей, используется стандартная процедура входа в систему по паролю.

Все биометрические эталоны пользователей хранятся в ОС в дополнительном защищенном хранилище, а информация о пользователях – в системном защищенном хранилище SAM (Security Accounts Manager). Использование дополнительного защищенного хранилища для биометрических эталонов вызвано особенностями архитектуры ОС Windows 2000/2003/XP. На эффективность работы системы, в целом, это не повлияло.

Работа поддержана грантом РФФИ № 06-07-96609-р_юг_а

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Широчин В.П., Кулик А.В., Марченко В.В. Динамическая аутентификация на основе анализа клавиатурного почерка. – http://www.masters.donntu.edu.ua/2002/fvti/-aslamov/files/bio_autentification.htm.
2. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений: – Пенза: изд-во ПГУ, 2000. – 188 с.
3. Брюхомицкий Ю.А., Казарин М.Н. Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложения Хаара и меры близости Хэмминга / Известия ТРТУ. Тематический выпуск «Материалы V международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2003. - № 4(33). – С. 141-149.
4. Брюхомицкий Ю.А., Казарин М.Н. Скрытный клавиатурный мониторинг. Материалы VIII Международной научно-практической конференции «Информационная безопасность». – Таганрог, 2006.
5. Иванов А.И. Биометрические и нейросетевые механизмы связи с криптографическими механизмами информационной безопасности / Труды научно-технической конференции «Безопасность информационных технологий». - Секция 9. - Том 4. – Пенза, 2003. - С. 3-6.
6. Winlogon and GINA. Platform SDK: Authentication. http://msdn2.microsoft.com/en-us/library/aa380543.aspx
7. Пахомов С. Защита паролей Windows – платформ. Компьютер Пресс №4, 2006.

Материал поступил в редакцию 22.01.08

BRUICHOMICKI J.A., KAZARIN M.N. It is a lot of the factor system password - keyboard authentication

In job the basic classes of used now systems authentication, their advantages and lacks are briefly considered. In a class of biometric systems the using dynamic characteristics of the person, are especially selected keyboard systems authentication (KSA), which are most simple in realization, but has a high level of mistakes. The basic methods of representation of parameters and principles of functioning KSA are considered. With the purpose of decrease of a level of mistakes it is offered to hide to build KSA in the regular password system authentication. The formed thus password -keyboard system authentication (PKSA) combines at once three factors of protection: feature of keyboard input of the user, secret password of a phrase of the user and secret of the fact of presence of the biometric control. The level of mistakes PKSA becomes proportional to the best biometric systems. As a prime step of realization it is offered to use PKSA in personal and mobile computers. The development PKSA as software BioKeyProtect, focused on OS Windows 2000/2003/XP is described.

УДК 004.5;621.38

Воронов А.А.

АЛГОРИТМЫ ПОКРЫТИЯ ПРЯМОУГОЛЬНИКАМИ ОБЪЕКТОВ ТОПОЛОГИИ МИКРОСХЕМ

Введение. При производстве интегральных схем, фотоэлектрических преобразователей, ЖК-индикаторов, а также многих других микроэлектронных устройств возникает задача формирования топологических структур на металлизированных фотошаблонах. Эти структуры формируются с помощью специальных генераторов изображений. Особенностью этих генераторов является то, что они способны формировать лишь ограниченный спектр структур. Для создания произвольных топологических структур необходимо найти покрытие исходной структуры совокупностью более простых структур, которые может сформировать генератор изображений. Топологические структуры описываются многоугольниками. Генераторы изображений чаще всего формируют прямоугольники. Следовательно, задача формирования фотошаблона сводится к задаче покрытия произвольного многоугольника совокупностью прямоугольников [1].

Данная задача не является новой. Разработаны эффективные методы ее решения [1], однако при проектных нормах меньше 1 мкм возникают значительные трудности при генерации изображений, так как возрастает объем топологии и ее сложность. Поэтому разработка новых методов решения задачи покрытия прямоугольниками объектов топологии микросхем является актуальной. Одним из подходов к решению этой задачи являются переборные алгоритмы, они просты в реализации, но оказываются эффективными лишь при покрытии односвязных и небольших по числу угловых точек контуров многосвязных областей. Другим подходом являются алгоритмы сканирующего типа, и хотя в общем случае разбиение, полученное в результате работы этого алгоритма, не является минимальным, но, что существенно, число прямоугольников такого разбиения лежит в тех же пределах, что и число прямоугольников минимального разбиения. Таким образом, алгоритмы сканирующего типа эффективны не только по быстродействию, но и по числу прямоугольников результирующего разбиения. Существуют также различные комбинации предыдущих методов. Так, для построения покрытия односвязной произвольной области вначале производится разбиение исходной области на трапеции, которые затем покрываются прямоугольниками. Эта задача решается переборным алгоритмом.

Многоугольник является некоторой областью плоскости. Эта область может быть представлена контуром. Контур задается цепочкой отрезков прямых, начало которой соединяется с ее концом.

Ниже под покрытием многоугольника понимается его разложение в совокупность прямоугольников, объединение которых совпадает с исходным многоугольником [2].

Среди объектов топологии микросхем выделяются такие объекты, как окружности, кольца, шины. Для них разрабатываются специальные алгоритмы покрытия, которые по сравнению с универсальными алгоритмами оказываются более эффективными как по быстродействию, так и по качеству решения.

В настоящей работе рассматривается задача покрытия объектов топологии микросхем типа шины [1] и предлагаются алгоритмы ее решения. Предлагаемые алгоритмы реализованы на языке C++. Приводятся результаты экспериментальных исследований этих алгоритмов на реальных примерах.

1. Постановка задачи. Шина – это электрический проводник в виде металлической полосы, применяемый в микросхемах для передачи электроэнергии или информационных сигналов. Графически шина может быть представлена ломаной с постоянной ненулевой толщиной. Соответственно, шина задается трассой в виде ломаной и шириной этой трассы. Трасса представляется в виде последовательности вершин: (x_1, y_1), (x_2, y_2), …, (x_k, y_k). Вершина с номером i $(1 \le i \le k)$ в этой последовательности задается координатами x_i, y_i. Каждая соседняя пара вершин (x_j, y_j), (x_{j+1}, y_{j+1}) этой последовательности, где $(1 \le j < k)$, задает отрезок прямой. Таким образом, данная последовательность вершин задает последовательность отрезков, из которых и состоит трасса.

По трассе шины и ее ширине можно найти точки контура многоугольника, задающего эту шину.

Будем говорить, что прямоугольник принадлежит многоугольнику, если любая точка плоскости, находящаяся внутри или на границе этого прямоугольника, находится внутри или на границе многоугольника.

Прямоугольник называется *d*-допустимым, если длина любой из его сторон не превышает некоторой величины *d*, где *d* является положительным вещественным числом.

Точка плоскости *r*, находящаяся внутри или на границе многоугольника, называется *d*-покрываемой, если существует *d*-допустимый прямоугольник, принадлежащий данному многоугольнику, такой, что точка *r* находится на границе или внутри данного прямоугольника.

Заметим, что в многоугольнике могут существовать точки, расположенные около острых углов, которые не являются *d*-покрываемыми. Так, точка плоскости, находящаяся в вершине острого угла, не является *d*-покрываемой для любой величины *d*.

Под покрытием многоугольника понимается совокупность *d*-допустимых прямоугольников, удовлетворяющих следующим условиям:

- всякий прямоугольник из данной совокупности принадлежит данному многоугольнику,
- для всякой *d*-покрываемой точки *r* многоугольника найдется хотя бы один прямоугольник этой совокупности такой, что точка *r* находится на границе или внутри данного прямоугольника [3].

В настоящей работе рассматривается следующая задача.

Необходимо найти для шины, заданной трассой и шириной трассы *s*, покрытие, состоящее из минимального числа *d*-допустимых прямоугольников.

Прямоугольники в покрытии, как правило, пересекаются между собой. Важной характеристикой покрытия является сумма площадей пересечений прямоугольников в нем. Чем эта величина меньше – тем лучше. Вычисление этой характеристики является сложной задачей, поэтому она на практике не используется, однако при выборе метода решения задачи покрытия предпочтение отдается методу, позволяющему находить покрытие, в котором сумма площадей пересечений прямоугольников была бы наименьшей.

***Воронов Александр Анатольевич**, младший научный сотрудник Объединенный институт проблем информатики НАН Беларуси. Беларусь, 220012, г. Минск, ул. Сурганова 6, sash_v_oo@.tut.by*