Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

М.Н. Бобов

МЕТОДЫ ОПОЗНАНИЯ ПОЛЬЗОВАТЕЛЕЙ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

УЧЕБНОЕ ПОСОБИЕ
по курсам «Защита информации в банковских технологиях»,
«Защита программного обеспечения и баз данных в сетях телекоммуникаций",
«Криптографическая защита информации в телекоммуникациях»
для студентов специальности 45 01 03 «Сети телекоммуникаций»
дневной и заочной форм обучения

Минск 2004

УДК 681.324(075.8)
ББК 32.973 я 73
Б 72

Р е ц е н з е н т:
доцент кафедры радиотехнических систем БГУИР А.И. Митюхин

Бобов М.Н.

Б 72 Методы опознания пользователей в вычислительных сетях: Учеб. пособие по курсам «Защита информации в банковских технологиях», «Защита программного обеспечения и баз данных в сетях телекоммуникаций", «Криптографическая защита информации в телекоммуникациях» для студ. спец. 45 01 03 «Сети телекоммуникаций» дневной и заочной форм обуч./ М.Н. Бобов.– Мн.: БГУИР, 2004. – 20 с.: ил.
ISBN 985-444-686-7

В учебном пособии рассмотрены методы опознания пользователей в вычислительных сетях и приведена их классификация. Изложены принципы построения устройств опознания, дана их сравнительная характеристика, проанализированы режимы работы и изложены рекомендации по их использованию.

УДК 681.324(075.8)
ББК 32.973 я 73

ISBN 985-444-686-7

1. КЛАССИФИКАЦИЯ МЕТОДОВ ОПОЗНАНИЯ

Реализация процедур опознания пользователей, которые включают в себя идентификацию и проверку подлинности, является общей проблемой для любых систем, в которых требуется обеспечивать разграничение доступа к обрабатываемой информации. Так как функционирование всех механизмов разграничения доступа, использующих аппаратные или программные средства, основано на предположении, что любой пользователь системы представляет собой конкретное лицо, то должен существовать некоторый механизм его опознания, обеспечивающий установление подлинности данного пользователя, обращающегося к системе.

Существуют три класса опознания (рис.1), которые базируются:

а) на условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

б) на физических средствах, действующих аналогично физическому ключу (что имеет субъект);

в) на индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту).

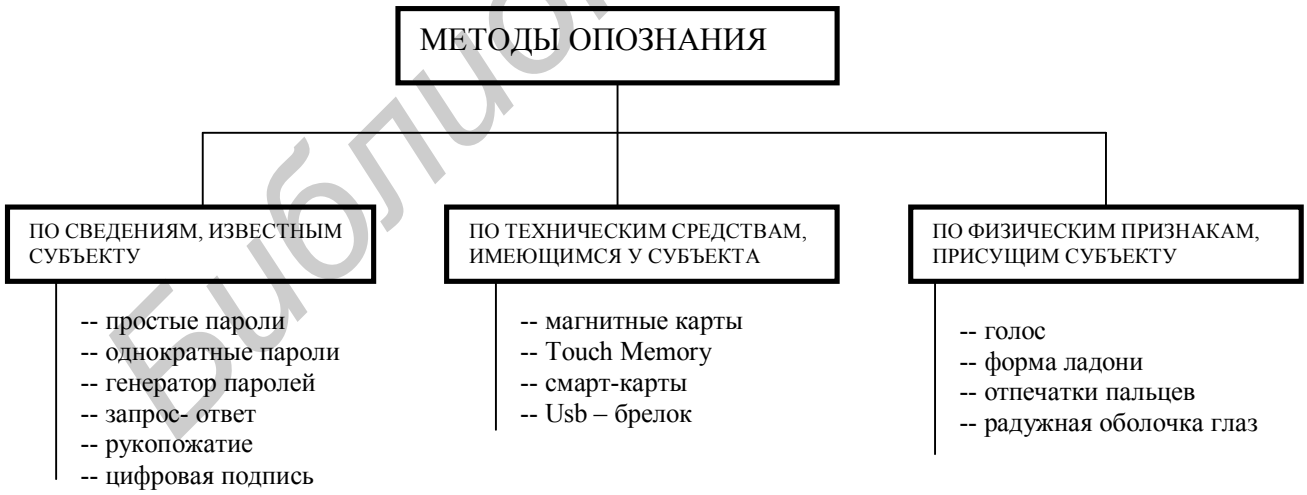

Рис.1. Классификация методов опознания

2. ОПОЗНАНИЕ НА ОСНОВЕ ПРИНЦИПА "ЧТО ЗНАЕТ СУБЪЕКТ"

К этому классу опознания относятся: метод паролей, метод "запрос-ответ", метод "рукопожатия".

2.1. Метод паролей

Данный метод заключается в том, что пользователь на клавиатуре компьютера или специально имеющемся наборном поле набирает только ему известную комбинацию букв и цифр, являющуюся, собственно, паролем. Данный пароль сравнивается с эталонным, хранящимся в системе, и при положительном результате проверки пользователь получает доступ к системе. Данная схема опознания является простой с точки зрения реализации, так как не требует никакой специальной аппаратуры и реализуется посредством небольшого объема программного обеспечения.

Схема с простым паролем имеет два недостатка:

во-первых, для большинства пользователей сложно хранить в своей памяти произвольное число, используемое в качестве пароля;

во-вторых, пароль может быть легко использован другим лицом, так как его легко подсмотреть.

Модернизацией схемы простого пароля является пароль однократного использования. В этой схеме пользователю выдается список из N паролей, такие же N паролей хранятся в системе. Данная схема обеспечивает большую степень безопасности, но она является и более сложной. Здесь при каждом обращении к системе синхронно используется пароль с текущим номером, а все пароли с предыдущими номерами вычеркиваются. В случае, если старый пароль из предыдущего сеанса стал известен другому пользователю, система его не воспринимает, так как действующим будет следующий по списку пароль.

Схема паролей однократного использования имеет следующие недостатки:

пользователь должен помнить или иметь при себе весь список паролей и следить за текущим паролем;

в случае, если встречается ошибка в процессе передачи, трудно определить, следует ли передавать тот же самый пароль или послать следующий;

необходимо иметь разные таблицы паролей для каждого пользователя, так как может произойти рассинхронизация работы.

Последний недостаток можно устранить, используя генератор паролей. В этом случае в ЭВМ реализуется алгоритм, осуществляющий преобразование

$$F(x, k) = y,$$

где x, k, y – двоичные векторы соответственно характеристического номера, ключа и пароля.

Реализация процедуры опознания пользователя сводится к двум задачам: заготовке паролей и установлению подлинности.

При заготовке паролей с помощью преобразования $F(x, k) = y$ получают набор чисел

$$X_i^j, \Pi_i^j,$$

где i - номер пользователя; j - номер обращения данного пользователя; П – текущее значение пароля, сформированное на ключе k.

Полученный набор выдается соответствующим пользователям.

При опознании обращающийся к системе пользователь с номером i вводит парольный набор X_i^j, Π_i^j в ЭВМ. Программа опознания выделяет номер пользователя X_i^j, а также запоминает пароль Π_i^j. Для каждого i-го пользователя существует свой счетчик обращений S_i. В случае, если $j \le S_i$, программа выдает сообщение о несанкционированном доступе (НСД). В противном случае включается генератор паролей. Преобразование $F(x_i^j,к)$ на действующем ключе k выдает число y, которое сравнивается с паролем Π_i^j. В случае совпадения y и Π_i^j пользователь считается опознанным, а в случае несовпадения выдается сигнал о несанкционированном доступе.

Использование генератора паролей избавляет от необходимости хранить таблицы паролей для каждого пользователя, однако первые два недостатка при его использовании сохраняются.

2.2. Метод "запрос-ответ"

В методе "запрос-ответ" набор ответов на m стандартных и n ориентированных на пользователя вопросов хранится в ЭВМ и управляет программой опознания. Когда пользователь делает попытку включиться в работу, программа опознания случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Пользователь должен дать правильный ответ на все вопросы, чтобы получить разрешение на доступ к системе. Вопросы могут быть выбраны таким образом, чтобы пользователь запомнил ответы и не записывал их.

Модификация этого метода предполагает изменение каждый раз одного или более вопросов, на которые пользователь давал ответ до этого.

Существует два варианта использования метода "запрос-ответ", вытекающие из условий m = 0 или n = 0. Вариант с m = 0 предполагает, что вопросы составлены на основе различных фактов биографии индивидуального пользователя, представляют собой имена его друзей, дальних родственников, старые адреса и т.д. На опознавательный вопрос пользователь, который его сам предложил, всегда даст правильный ответ, что не сможет сделать злоумышленник. Иногда предпочтительнее вариант с n = 0, т.е. пользователям задается большее количество стандартных вопросов и от них требуются ответы на те, которые они сами выберут. Достоинство рассмотренной схемы в том, что пользователь может выбирать вопросы, а это дает весьма высокую степень безопасности в процессе включения в работу. В то же время нет необходимости хранить в системе тексты вопросов для каждого пользователя, достаточно хранить указатели на вопросы, выбранные данным пользователем, вместе с информацией, устанавливающей его подлинность. Текст каждого стандартного вопроса необходимо ввести для хранения только один раз, поэтому в системе с большим числом пользователей это может дать экономию памяти.

Метод "запрос-ответ" наряду с достоинствами все же имеет недостатки, ограничивающие возможность его использования, а именно:

во-первых, он требует проявления изобретательности самих пользователей, что для них является дополнительной нагрузкой;

во-вторых, для большинства людей опознавательные вопросы и ответы, как правило, приобретают стереотипность, и весьма вероятно, что настойчивый нарушитель может, собрав статистику, предугадать многие вопросы и ответы;

в-третьих, метод требует обмена множеством опознавательных запросов и соответствующих им ответов, что для пользователей может быть сложным и утомительным;

в-четвертых, в силу некоторой громоздкости метод "запрос-ответ" может удачно использоваться только для небольших организованных групп пользователей и неприменим для массового использования.

2.3. Метод "рукопожатия"

Для исключения некоторых недостатков описанных ранее методов опознания можно потребовать, чтобы пользователь установил свою подлинность с помощью корректной обработки алгоритмов. Это часто также называют процедурой опознания в режиме "рукопожатия", и она может быть выполнена как между двумя ЭВМ, так и между пользователем и ЭВМ. Процедуры опознания в режиме "рукопожатия" обеспечивают большую степень безопасности, чем многие другие схемы, но вместе с тем являются более сложными и требующими дополнительных затрат времени для пользователя. В процессе "рукопожатия" пользователь должен обменяться с алгоритмом последовательностью паролей (команд), которые должны быть названы правильно и в правильной последовательности, хотя сам пользователь не знает алгоритма. Правильное завершение алгоритма подтверждает подлинность пользователя.

Другой вариант метода "рукопожатия" заключается в следующем. Для установления подлинности ЭВМ выдает пользователю число, выбранное случайным образом, а затем запрашивает от него ответ. Для подготовки ответа пользователь А применяет собственное, заранее подготовленное преобразование F_A. Информацией, на основе которой принимается решение, здесь является не пароль, а преобразование F_A. ЭВМ посылает значение X, а пользователь отвечает значением $F_A(X)$. Любое постороннее лицо для проникновения в систему даже в случае знания значений X и $F_A(X)$ должно тем не менее отгадать функцию преобразования на основе нескольких вводов и выводов, так как сама функция преобразования никогда не передается по линиям связи, по которым

посылаются только X и $F_A(X)$. Эта схема удобна для работы в некоторых сетях ЭВМ, так как необходимые вычисления довольно просты и никакие пароли не нужно помещать на хранение. Кроме того, функция преобразования может быть различной для каждого пользователя, что позволяет однозначно идентифицировать каждое лицо, обращающееся к системе.

Функцию преобразования можно изменять в зависимости от некоторого внешнего события. Например, в случае, когда удаленный пользователь обращается к защищенному компьютеру, программа опознания обращается к таймеру ЭВМ. Несколько последних значений цифр, содержащихся в таймере, суммируются с паролем и записываются в память. Содержимое таймера посылается удаленному пользователю. Пользователь суммирует пароль с цифрами таймера и передает результат обратно в ЭВМ, где эта сумма сверяется с суммой, хранящейся в памяти.

Способ "рукопожатия" более труден для раскрытия, чем пароль, но сложнее в реализации. В отличие от паролей преобразование никогда не появляется в линиях связи, однако в силу своей неизменности, также может быть достаточно просто определено. Основным недостатком метода "рукопожатия" является временная задержка, выражающаяся в необходимости, как и в методе "запрос-ответ", организации обмена несколькими сообщениями между пользователем и системой в процессе опознания.

3. ОПОЗНАНИЕ НА ОСНОВЕ ПРИНЦИПА "ЧТО ИМЕЕТ СУБЪЕКТ"

К этому классу опознания относятся методы, основывающиеся на физических средствах, которые имеет при себе данный пользователь, обращающийся к системе. К ним относятся электромеханические и электронные ключи, идентификационные карты с перфорированным или магнитным кодом и другие подобные средства, которые можно объединить общим названием "физический ключ". В силу того, что для надежной защиты ключ должен иметь множество возможных значений, которые в процессе эксплуатации должны в произвольный момент изменяться, электромеханические ключи и перфокарточки мы рассматривать не будем, а обратимся к магнитным картам и электронным ключам.

3.1. Идентификационные магнитные карты

В магнитных картах информация записывается на нескольких дорожках магнитного слоя и представляет собой данные, используемые для идентификации. К этим данным относятся: номер пользователя или его имя, пароль, количество допустимых использований карты и т.д. Наряду с очевидной простотой использования магнитные карты обладают низкой защищенностью от копирования содержимого. Для защиты от копирования магнитные карты снабжаются различными защитными средствами. Один из методов состоит в нанесении магнитного слоя обычного типа поверх второго слоя с более высокой коэрцитивной силой, т.е. для изменения состояния первого слоя требуется более сильное магнитное поле. В этом случае обычными методами невозможно считать или изменить запись нижнего слоя. Считывающее устройство, читая карту, содержащую идентификатор, вначале создает поле, стирающее любую запись, сделанную обычным способом, а затем уже считывает лежащую ниже "твердую" запись, в которой действительно находится информация.

В другом методе используется постоянная магнитная разметка ленты, которая наносится в процессе ее производства. Метод, известный под названием "влажной разметки", состоит в определенной ориентации осей ферромагнитных кристаллов до момента, пока наполнитель еще не высох, причем селективная ориентация осей кристаллов в различных частях ленты создает магнитную запись, которую никак нельзя изменить. Чтобы прочесть эту запись, кристаллы необходимо подвергнуть воздействию постоянного магнитного поля с определенной ориентацией. Изменение положения кристаллов вдоль ленты будет наводить внешнее поле, которое можно прочитать с помощью обычных, удобно расположенных головок. Изготовленные таким образом идентификационные карточки могут обеспечить "уникальную" идентичность, которую трудно подделать, поскольку для этого требуется овладеть технологией производства магнитных покрытий и влажной разметки.

Таким образом, для осуществления защиты от подделки или копирования магнитной карточки требуются сложная технология их изготовления и соответственно сложная аппаратура для считывания записанной на них информации. Следует отметить, что при любых способах достичь абсолютной защиты от ко-

пирования магнитных карт практически невозможно, так как носитель всегда открыт для доступа посторонних лиц.

3.2. Электронные ключи

Электронный ключ в самом общем смысле представляет собой физический носитель секретного кода, являющегося аутентификатором пользователя. В отличие от парольных систем при использовании электронного ключа (ЭК) пользователь имеет ряд преимуществ:

во-первых, ему не надо запоминать значение пароля, так как пароль записан в ключе;

во-вторых, он освобожден от проблемы защиты пароля от компрометации при его вводе, так как пароль считывается из ключа;

в-третьих, все функции по защите от подделки пароля или его несанкционированного использования (метод разовых паролей, метод "рукопожатия") возлагаются на электронный ключ;

в-четвертых, секретный код можно сделать сколь угодно большим, так как пользователь с ним непосредственно не работает.

В силу того, что, как и идентификационная магнитная карта, электронный ключ является физическим средством хранения аутентификатора пользователя, его можно скопировать и подделать. В основном все многообразие электронных ключей классифицируется по основному признаку, определяющему их защищенность от копирования и подделки секретности, так как быстродействие, объем хранимого идентификатора, габариты и другие характеристики являются, по существу, производными от него.

Ключ, который невозможно подделать, является, как правило, активным устройством, содержащим в памяти секретный код, недоступный для чтения. Устройство можно сконструировать таким образом, что попытка прочесть ключ приводит к его уничтожению. Устройство такого типа обладает "индивидуальностью", которую можно выявить только посредством задания устройству различных цифровых значений и записи его ответов.

Электронный ключ может использоваться локально, подобно ключу от дверного замка, или на расстоянии, например для опознания удаленных пользователей, обращающихся к ЭВМ. Для своего восприятия электронный ключ

должен взаимодействовать с "замком" (ответной частью), запрашивающим ключ и проверяющим его идентичность. Вначале идентичность необходимо определить каким-либо независимым способом, чтобы ввести в действие замок, отвечающий данному ключу. Затем замок посылает набор цифр к ключу и запоминает его ответы. Впоследствии, когда ключ действительно используется для опознания пользователя, некоторые из этих цифровых наборов повторяются в качестве опознавательных вопросов к ключу, а ответы сравниваются с уже хранящимися в памяти. Если опознание осуществляется многократно, то замок может послать новые цифровые комбинации, которые добавляются к списку опознавательных вопросов и ответов.

Один и тот же ключ может подходить к нескольким замкам, и один и тот же замок может отвечать нескольким ключам, не нарушая при этом секретности ни замка, ни ключа. Однако, если имеется возможность перехвата всех опознавательных вопросов и ответов для данного замка, то ключ можно подделать. Такой поддельный ключ может приниматься как подлинный во всех последующих сеансах опознания до тех пор, пока он не будет выявлен новыми опознавательными вопросами. Используя большое число ответов и создавая каждый раз новые, можно повысить уровень защиты, однако более надежным способом является применение методов шифрования для защиты передаваемых идентификаторов от удаленных абонентов в ЭВМ.

Независимо от сферы использования электронный ключ (рис.2) содержит в своем составе узел памяти для хранения секретного кода, узел преобразования для обеспечения безопасной передачи кода ключа за пределы электронного ключа, а также узел сопряжения для соединения и обеспечения интерфейса с ответной частью (ОЧ). Ответная часть, являясь, как указывалось выше, обязательным элементом электронного ключа, содержит помимо перечисленных выше узлов узел питания и синхронизирующий блок для задания программы работы электронного ключа.

Рассмотрим требования, которым должны удовлетворять указанные узлы при реализации.

Требование 1. Для хранения секретного пароля ключ содержит элемент памяти. Поэтому требование защиты от несанкционированного доступа к ключу обуславливает требование защиты элемента памяти от ознакомления с его содержимым. Полагая, что ключ защищен от тривиального тестирования эле-

мента памяти (прозвонки) со стороны внешнего соединителя, возможность считывания содержимого элемента памяти может быть достигнута только посредством вскрытия ключа, т.е. нарушения его физической целостности.

Рис. 2. Структурная схема электронного ключа

Наиболее приемлемыми для хранения кодов в ЭК в настоящее время являются энергонезависимые запоминающие устройства. Они обладают большой емкостью, имеют малые габариты, невысокую стоимость и соответствуют требованиям, предъявляемым к аппаратуре специального назначения. Однако простых средств для оперативного уничтожения информации, хранимой в данных запоминающих устройствах, в настоящее время не существует. Поэтому единственным пока методом, обеспечивающим защиту от непосредственного дос-

тупа к элементу энергонезависимой памяти, является неразъемность конструкции ЭК.

Требование 2. Кроме защиты от НСД электронный ключ должен быть защищен от копирования, а следовательно, от подделки. Для этих целей он содержит узел преобразования, который должен выдавать на любое входное воздействие практически случайную выходную последовательность, по структуре которой истинное значение секретного кода было бы невозможно вскрыть. Следовательно, узел преобразования должен представлять собой криптосхему, реализующую один из криптостойких алгоритмов преобразования данных.

Требование 3. Кроме использования криптосхемы для защиты от копирования диалог между ЭК и ответной частью должен быть реализован таким образом, чтобы без предварительного установления их соответствия секретный код из ключа не выдавался в ответную часть.

Следовательно, сам ключ как средство, хранящееся у пользователя и доступ к которому проконтролировать чрезвычайно трудно, должен выдавать правильное значение секретного кода только после установления правильности запроса со стороны ответной части. С другой стороны, ответная часть также должна быть защищена от НСД к кодам, которыми она обменивается с ключом. Для защиты от прочтения кодов ОЧ она должна содержать в своем составе генератор случайных чисел (ГСЧ), с помощью которого маскируются коды, выдаваемые из ОЧ. В этом случае на ее выходе всегда будут появляться случайные последовательности, по значениям которых невозможно сделать вывод о структуре требуемых запросов.

Секретность электронного ключа, как и всех устройств опознания, относящихся ко второму классу, определяется выражением

$$P_{СК} = 1 - (1 - P_Н)(1 - P_П)(1 - P_У),$$

где $P_Н$ - вероятность несанкционированного копирования секретных параметров ключа;

$P_П$ - вероятность подбора входных воздействий;

$P_У$ - вероятность подбора выходных воздействий.

Обратной величиной секретности является вероятность подделки, которая определяется по формуле

$$P_К = 1 - P_{СК}.$$

Для уменьшения вероятности подделки и с учётом выполнения изложенных выше требований при разработке устройств опознания используются следующие механизмы:

1) ограничение попыток НСД;

2) контроль цикла работы;

3) маскирование выходных сообщений.

При использовании первого механизма ограничивается количество возможных попыток ввода неправильных кодов аутентификации. В этом случае при допустимом числе попыток К вероятность подбора входных воздействий $P_П$ равна:

$$P_П = 1 - \prod_{i=1}^{k} (1 - P_{пi}) = \frac{K}{N},$$

где N - объем входного алфавита.

Так как $K << N$ и $K = const$, то при использовании этого механизма получаем выигрыш в защите.

Реализация механизма контроля цикла работы заключается в том, что устройство опознания функционирует по заранее установленным жестким циклам и ни при каких входных воздействиях такая цикличность его работы не нарушается. В результате устройство опознания, во-первых, реагирует только на заранее определённую последовательность входных сообщений, а все остальные сообщения игнорируются. Во-вторых, все выходные сообщения из устройства выдаются только в заранее определенные моменты времени, когда процессы приема и обработки входного воздействия полностью завершены. Так как цикл работы жестко задан, всегда можно ввести определенную задержку по времени его выполнения таким образом, чтобы повысить безопасное время секретного кода, которое определяется по формуле

$$T_б = W \cdot T_ц = W(t_р + \tau),$$

где W — количество операций, которые необходимо выполнить для подбора секретного кода;

t_p - время непосредственной работы;

τ - задержка по циклу.

При маскировании выходных сообщений алфавит выходных сообщений должен быть многоальтернативным, т.е. таким, чтобы в процессе осуществления попыток компрометации ключа невозможно было установить соответствие между входными и выходными сообщениями. Реализация механизма обеспечивается использованием ГСЧ и криптосхемы.

4. ОПОЗНАНИЕ НА ОСНОВЕ ПРИНЦИПА "ЧТО ПРИСУЩЕ СУБЪЕКТУ"

Данный принцип опознания базируется на определении индивидуальных характеристик, присущих каждому пользователю и позволяющих выделить его среди других лиц. К наиболее широко используемым персональным характеристикам относятся голос, личная подпись, форма ладони и отпечатки пальцев. В последнее время появилось еще несколько методов физического опознания - по структуре сетчатки глаз, сопротивлению определенных участков кожи, запаху тела и др. В каждом случае способ опознания состоит в измерении индивидуальных характеристик и вычислении индексов, аналогичных характеристическим параметрам распознавания образов, которые можно передать в центральную ЭВМ для сопоставления с набором индексов, хранящихся в памяти ЭВМ и взятых непосредственно у интересующего лица.

4.1. Параметры идентификации физических признаков

Механизм опознания личной подписи может измерять число касаний и отрывов пера от бумаги, среднюю вертикальную скорость движения пера, число вертикальных отклонений и множество других подобных параметров. Эти характеристики могут быть самыми разнообразными, однако не все из них являются независимыми, и задача состоит в том, чтобы выбрать хороший набор характеристик с достаточно малой взаимной корреляцией. Проверка подлинности подписи зависит от движения пера, которое нельзя воспроизвести по виду подписи, зафиксированной на бумаге. Это почти полностью исключает воз-

можность подлога, так как искусство тех, кто профессионально подделывает подписи, основано на внешнем виде почерка. Набор измеряемых характеристик должен сохраняться в тайне, так как их знание может привести к подделке подписи посредством тренировки в копировании измеряемых характеристик. Как показала практика, это очень сложная задача.

Аналогичные особенности характерны и для других методов опознания этого класса. Например, некоторые устройства, определяющие форму ладони, измеряют прозрачность тканей кожи между пальцами для защиты от подлогов с помощью картонных шаблонов. Механизмы, построенные на анализе отпечатков пальцев, используют мельчайшие детали в виде разветвлений, окончаний и пробелов в линиях на кончиках пальцев. Так как в каждом отпечатке содержится множество таких отличий, измеряемые характеристики могут базироваться на выбранном наборе деталей. Системы распознавания речи, основанные на анализе спектрограммы голоса пользователя, можно защитить от использования магнитных записей вместо голоса законного обладателя с помощью метода опознавательных вопросов и ответов. При этом ЭВМ будет требовать от абонента повторения определенного набора слов.

4.2. Особенности опознания по физическим признакам

Значения характеристик, получаемых в процессе работы средств опознания по физическим признакам, всегда имеют разброс в небольшой области с некоторым вероятностным распределением, поэтому для принятия решения необходимо определить "окно приемлемости" для каждого параметра. При экспериментальной оптимизации качества механизма опознания размер ″окна″ может меняться, но он всегда остается больше некоторого минимума, так как практически не существует абсолютно надежного набора параметров для опознания по физическим признакам. Если взять слишком широкое значение ″окон″, то можно принять любой запрос, а если очень узкое, то на все попытки последует отказ, в том числе и на запросы законных пользователей. На рис.3 представлены типичные кривые, показывающие соотношение между ошибками этих двух типов.

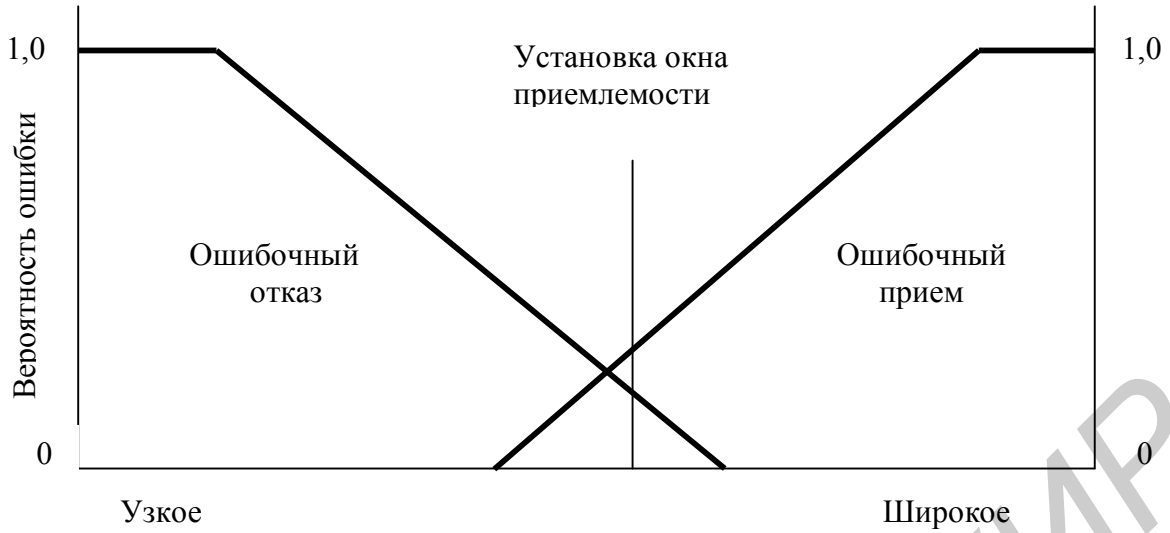

Рис. 3. Два вида ошибок при опознании по индивидуальным характеристикам

На практике, как видно из рисунка, оба типа ошибок нельзя свести к нулю одновременно независимо от величины установленного порога. В этом – коренное отличие последнего класса систем опознания от первых двух, где опознание считается установленным только после абсолютного совпадения предъявленного аутентификатора.

В системе опознания по физическим признакам всегда обязательно наличие процедуры распознавания образов и качество опознания напрямую зависит от качества реализации этой процедуры. Система опознания собирает от пользователей набор значений параметров, который служит для образца, и определяет положения и размеры «окон». В нее может быть заложена возможность совершенствования в процессе накопления опыта опознания пользователей. Если выбирается слишком высокое значение «окон», то возможен прием любого запроса, а если - очень узкое, то на все попытки последует отказ, в том числе и на запросы законных пользователей. Целью процедуры распознавания образов является сведение к минимуму ошибок обоих типов. Процент ошибочных отказов можно уменьшить, если пользователю предоставить возможность выполнить процедуру идентификации более одного раза, причем успех любой из попыток принимается как достаточное условие для подтверждения личности. Ясно, что эта процедура вместе с тем увеличивает вероятность ошибочного опознания. Использование метода опознания по физическим признакам при опознании лица, не известного заранее, является практически не осуществимым, так как это требует выработки критериев оценки персональных характе-

иртик, чтобы выделить одного индивидуума среди всех других, обслуживаемых данной системой. Хотя физические параметры содержат достаточную информацию для опознания отдельного лица, эта процедура основывается на очень тщательном изучении хорошо измеренных параметров и выделении всех их особенностей. При практической же реализации данного метода опознание осуществляется на основе значительно меньшего объема информации и служит только для проверки характеристик одного, предположительно известного лица посредством сопоставления с соответствующей записью, хранящейся в памяти ЭВМ и составленной на основе ранее выполненных измерений его характеристик.

Таким образом, методы опознания, основанные на определении характеристик личности пользователя, более сложны и дороги при реализации, чем методы, основанные на использовании паролей и физических ключей, так как, во-первых, необходимо осуществлять довольно сложную процедуру распознавания и сравнения образов. Кроме того, в них значительно более вероятен отказ в доступе действительному пользователю из-за ошибок самой системы, а необходимость сбора характеристик и установления подлинности пользователя до того, как он обратится к системе, делает эти методы неудобными и малопригодными для распределенных систем с большим количеством пользователей.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАЧИ

1. Пояснить сущность и особенности классов опознания пользователей в вычислительных сетях.

2. Разработать алгоритм опознания пользователей на основе метода ″рукопожатия″.

3. Какие требования предъявляются к элементам электронных ключей при их реализации?

4. Определить вероятность подделки электронного ключа для следующих параметров: $K = 10$, $N = 2^{32}$, $P_H = 10^{-5}$, $P_У = 10^{-6}$.

5. Почему методы опознания по физическим признакам мало пригодны для распределенных систем с большим количеством пользователей?

ЛИТЕРАТУРА

1. Бобов М.Н., Конопелько В.К. Обеспечение безопасности информации в телекоммуникационных системах. – Мн.: БГУИР, 2002. – 164 с.

2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем.- М.: Горячая линия - Телеком, 2000. – 452 с.

3. Бабенко Л.К., Ищуков С.С., Макаревич О.Б. Защита информации с использованием смарт-карт и электронных брелоков.- М.: Гелиос АРБ, 2003. – 352 с.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. 2-е изд. - М.: Радио и связь, 2002. – 328 с.

5. Стенг Д., Мун С. Секреты безопасности сетей. - Киев.: Диалектика, 1996. – 544 с.

Св. план 2004, поз.109

Учебное издание

Бобов Михаил Никитич

МЕТОДЫ ОПОЗНАНИЯ ПОЛЬЗОВАТЕЛЕЙ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

УЧЕБНОЕ ПОСОБИЕ
по курсам «Защита информации в банковских технологиях»,
«Защита программного обеспечения и баз данных в сетях телекоммуникаций",
«Криптографическая защита информации в телекоммуникациях»
для студентов специальности 45 01 03 «Сети телекоммуникаций»
дневной и заочной форм обучения

Редактор Н.А. Бебель

Подписано в печать		Формат 60x84 1/16.
Бумага офсетная.	Печать ризографическая.	Усл.печ. л.
Уч.-изд. л. 1,0.	Тираж 50 экз.	Заказ 224.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия на осуществление издательской деятельности №02330/0056964 от 01.04.2004.
Лицензия на осуществление полиграфической деятельности №02330/0133108 от 30.04.2004.
220013, Минск, П. Бровки, 6