УДК 004.052.42

МАРКОВСКИЙ А.П.,
АБУ УСБАХ А.Н.,
АЛЬМУРАДИ В.М.

ОРГАНИЗАЦИЯ ИДЕНТИФИКАЦИИ АБОНЕНТОВ МНОГОПОЛЬЗОВАТЕЛЬСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ АППАРАТНО ЗАЩИЩЕННОЙ ПАМЯТИ

Разработана новая двухуровневая организация идентификации удаленных пользователей, которая использует один цикл передачи между пользователями и системой. Предложенная схема не использует списка паролей зарегистрированных пользователей и операций поиска и соответственно не накладывает ограничений на число пользователей. Объем информации, используемой при идентификации в предложенной схеме существенно меньше в сравнении с известными схемами. Это позволяет использовать аппаратно защищенную энергонезависимую память для хранения идентификационной информации и таким путем уменьшить риск незаконного доступа к ресурсам системы.

The new two-level organization of identification of remote abonent, which requires one communication between users and verifiers in system, has been proposed. Presented organization does not imply the password list of the legal users and searching operations and correspondingly does not impose restrictions on the number of users. The information capacity to be stored in secret is much less in the proposed identification scheme as compared to the known ones. This allows using hardware-based secure active low-capacity nonvolative memory for storing identification information and such way impair the risk of illegal access to system resources.

Введение

Развитие интегрированных систем обработки информации в значительной степени зависит от эффективности реализации в них функций защиты информации и разделения прав доступа к данным. Важное место в арсенале средств защиты интегрированных информационных и вычислительных ресурсов от несанкционированного доступа играет идентификация абонентов многопользовательских систем.

Расширение использования интегрированных систем хранения и обработки информации сопряжено с увеличением риска несанкционированного доступа к их ресурсам. Это обусловлено, с одной стороны, ростом технических возможностей для реализации несанкционированного доступа, а с другой – увеличением потенциальных выгод от такого доступа.

В этих условиях необходимо адекватное совершенствование всего арсенала средств, исключающих несанкционированный доступ к информационным и вычислительным ресурсам, в том числе и средств идентификации абонентов многопользовательских систем. Особую остроту в современных условиях приобретает проблема защиты от несанкционированного доступа к интегрированным системам компьютеризированного управления сложными техническими объектами.

Таким образом, проблема повышения эффективности идентификации удаленных абонентов многопользовательских систем является актуальной и важной для современного этапа развития информационных технологий.

Анализ проблемы эффективности идентификации абонентов

Эффективности идентификации удаленных абонентов пользователей определяется двумя факторами: устойчивостью к попыткам незаконного доступа (измеряется объемом затрат ресурсов, требующимися для такого доступа) и объем ресурсов, затрачиваемых для идентификации. Очевидно, что указанные факторы являются взаимосвязанными: чем выше уровень надежности идентификации абонента, тем сложнее ее процедура и тем больше ресурсов требуется для реализации процесса идентификации. С другой стороны, многопользовательские системы являются системами массового обслуживания и, соответственно, должны обладать производительностью, обеспечивающей возможность обработки запросов большого числа абонентов без существенных задержек. Фактически зависимость между рассматриваемыми факторами эффективности носит более сложный характер, поскольку результативность ряда способов незаконного доступа к ресурсам прямо зависит от времени

идентификации абонентов [2]. Следовательно, высокая эффективность идентификации абонентов может быть достигнута только в рамках разрешения компромисса между надежностью и скоростью идентификации.

В основе большинства существующих систем идентификации удаленного абонента лежит концепция доказательства знания им какой-то информации. Соответственно, схема идентификации включает два этапа: регистрацию абонента, во время которой абонент обретает идентифицирующую информацию и собственно идентификацию, в рамках которой осуществляется проверка легальности доступа.

К настоящему времени созданы и активно используется большое число протоколов идентификации удаленных абонентов [1,2]. Обычно выделяют два базовых подхода к идентификации: с использованием паролей и на основе концепции нулевого знания. Идентификация на основе концепции нулевого знания считается строгой, однако существующие методы ее реализации требуют больших вычислительных ресурсов [2]. Именно поэтому, идентификация на основе паролей широко используется во многих системах.

Для получения несанкционированного доступа, нарушитель может выполнить чтение, перехват и подмену информации, используемой в процессе идентификации при ее передаче по открытых линиях. Кроме того, потенциальную опасность представляет возможность доступа к информации, используемой для предоставления прав доступа со стороны самой системы [2].

Одним из наиболее потенциально опасных факторов риска для многопользовательских систем является возможность получения несанкционированного доступа к их ресурсам посредством чтения или изменения информации, используемой при идентификации легальных абонентов. Доступ к такой информации может быть осуществлен различными способами: с использованием специальных компьютерных вирусов, при “удачном” случайном входе в систему нелегального пользователя, а также легальным абонентом, пытающимся расширить свои права или предоставить возможность доступа к ресурсам системы нелегальным пользователям, и, наконец, недобросовестным лицом из персонала системы. Во всех перечисленных случаях доступ к информации, используемой при идентификации, осуществляется программным путем.

Существенным недостатком большинства известных схем идентификации абонентов является малая производительность, связанная с выполнением нескольких сеансов обмена информацией, а также необходимостью операций поиска по ключу. Невысокая скорость идентификации существенно ограничивает количество абонентов и не позволяет реализовать повторные сеансы идентификации непосредственно в процессе информационного обмена с тем, чтобы воспрепятствовать технологии доступа к ресурсам путем ”подмены легального абонента”.

Наиболее надежным способом сведения к минимуму или даже исключения возможности доступа сторонних лиц к информации, используемой для идентификации, является применение специальной энергонезависимой памяти, реализующей защиту хранящихся в ней данных на аппаратном уровне. СБИС такой памяти серийно выпускаются некоторыми фирмами. Микросхемы защищенной памяти способны не только хранить информацию, но и выполнять с ней операции, предусмотренные протоколами идентификации, чтобы исключить временное хранение и использование на программно-доступных узлах компьютерных систем.

Основным недостатком существующих СБИС защищенной памяти является относительно малый объем информации, который может в ней храниться, в то время, как с ростом числа абонентов объемы информации, используемые для их идентификации быстро растут. В работе [3] предложена схема идентификации, требующая для идентификации всех абонентов только один код. Однако использование такой схемы не защищает от доступа легальных абонентов к недозволенным им ресурсам системы. Достоинством этой схемы является изменяемость идентифицирующей посылки при каждом обращении к системы.

Исходя из этого, для эффективного использования аппаратных средств защиты идентификационной информации в многопользовательских системах необходимо разработать способы идентификации, не требующие хранения больших объемов идентификационной информации.

Структура аппаратно-защищенной памяти

Основным назначением аппаратно реализуемой защищенной памяти (ЗП) является хранение идентификационной информации и осуществление контроля доступа к ней. Память должна быть энергонезависимой, чтобы исклю-

чить риск доступа к хранящейся в ней информации в процессе ее записи.

В основу построения защищенной памяти положены следующие принципы:

1. Аппаратно реализуемая ЗП должна иметь открытый интерфейс подключения к стандартным шинам компьютеров, в частности к шине PCI. Конфигурирование ЗП и выделение ей адресного пространства должно выполняться в соответствии с технологией Plug and Play.

2. В ЗП хранится информация, которая является объектом защиты. Эта информация не должна записываться в ЗП и считываться из нее в явном виде.

3. ЗП кроме функций хранения информации должна реализовать операции криптографической обработки, в которой используется указанная секретная информация. Отсюда следует, что эффективность ЗП напрямую зависит от ее специализации: тем больше функций первичной обработки, связанной с секретной информацией будет выполнять ЗП, тем ее использование будет эффективнее в плане реализации функций защиты.

Структура защищенной памяти, ориентированной для использования в системах идентификации абонентов показана на рис.1.

При записи информации в накопитель, адрес поступает на входной интерфейс и фиксируется на регистре адреса. Сами данные, которые записываются в ЗП, маскируются кодом, который известен только главному администратору системы. Для маскирования используется операция побитового суммирования по модулю 2. Все коды масок, которые секретны и известны только администратору системы хранятся в постоянной памяти ЗП. При записи секретной информации необходимо задать адрес используемой маски. этот адрес фиксируется на регистре адреса маски. Соответственно, из постоянной памяти масок считывается секретный код маски. На блоке логических элементов XOR маска снимается с записываемого кода и последний записывается в память. Такой порядок записи исключает возможность перехвата секретной информации во время записи в защищенную память.

Аналогичный порядок маскирования используется и при задании данных, которые сравниваются в процессе идентификации с кодами, хранящимися в накопителе ЗП. Код, который необходимо сравнить с секретным идентифицирующим кодом, хранящимся в ЗП, маскируется администратором и подается на вход ЗП.

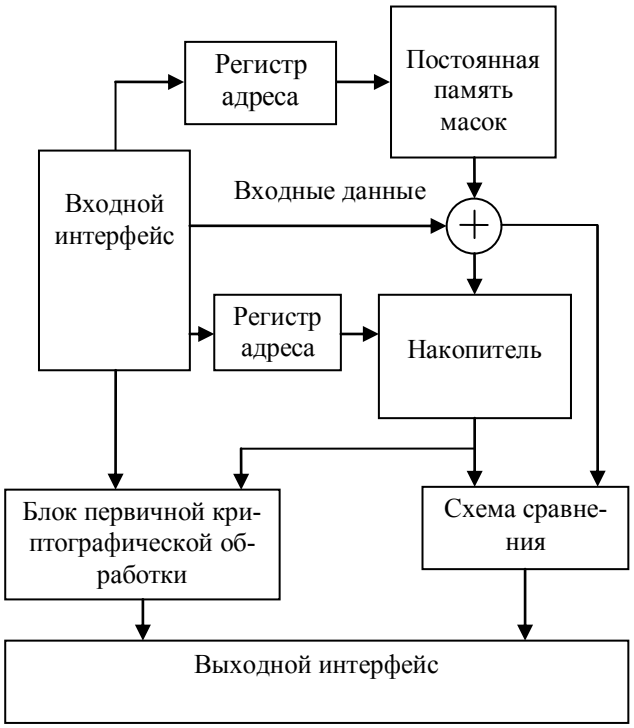

Рис.1. Структурная схема защищенной памяти, ориентированная для использования в системах идентификации абонентов

Внутри ЗП маска снимается. Одновременно на входной интерфейс подается адрес секретного кода, с которым производится сравнение. Этот секретный код считывается из накопителя и сравнивается с заданным кодом. Само сравнение осуществляется на аппаратном уровне внутри ЗП. Результат сравнения выдается в компьютер через выходной интерфейс.

Кроме операции сравнения аппаратные средства ЗП позволяют производить первичную обработку секретной информации при реалиизации криптографических алгоритмов защиты информации.

Двухуровневая схема идентификации абонентов многопользовательских систем

Высокая эффективность идентификации удаленных абонентов достигается как результат компромисса между противоречивыми требованиями. Сложность проблемы обусловлена невозможностью построения адекватной модели действий стороны, производящей попытку несанкционированного доступа. В первом приближении, процедура идентификации должна удовлетворять следующим требованиям:

1. Хранение идентифицирующей информации должна быть таким, что ее часть находится у абонента, а другая – в системе и каждая из час-

тей не была бы самодостаточной для доступа к ресурсам системы.

2. Пароль должен выбираться абонентом, не храниться в памяти, а вводиться при каждом сеансе и не быть достаточным для предоставления доступа к ресурсам.

3. Минимальное использование линий передачи данных – наиболее уязвимого места, с точки зрения незаконного проникновения к ресурсам системы;

4. Изменение идентифицирующей посылки абонента информации при каждом сеансе обращения к системе.

5. Объем сохраняемой в системе закрытой информации, которая используется для идентификации абонентов должен быть возможно меньшим.

6. Идентификационная информация при передаче по линии передачи данных должна шифроваться с использованием ключей, одинаковых для всех абонентов.

7. Распознавание легальных абонентов и сопоставление предоставляемых им прав доступа должно реализоваться разными механизмами защиты.

Приведенные требования сложно удовлетворить в рамках одноуровневой схемы. Поэтому целесообразным представляется разнесение этапа установления легальности абонента и установления прав доступа его к ресурсам системы в рамках двух разных уровнях идентификации. Такое разнесение реализовано в рамках разработанной организации идентификации абонентов многопользовательских систем.

Сущность предложенной двухуровневой организации идентификации абонентов состоит в том, что на первом уровне производится установление легальности абонента без использования системной информации, привязанной к конкретному пользователю. На втором уровне для идентификации абонента используются хранящиеся в системе данные, относящиеся к конкретному абоненту. Такой принцип использования идентифицирующей информации позволяет ускорить фильтрацию обращений к системе, связанных с попытками незаконного проникновения к ее ресурсам со стороны нелегальных пользователей.

В предлагаемой организации идентификации абонентов используются симметричное:

$$R = SCT(D,K)$$

и несимметричное (с открытым ключом):

$$R = NSCT(D,K_D)$$

криптографические преобразования (в качестве первого может, например, использоваться алгоритм Rijndael, а в качестве второго–RSA).

Через D обозначен блок данных до шифрования, а через R-после шифрования, K–ключ преобразования. Обратные преобразования обозначены как:

$$D = SCT^{-1}(R,K) \text{ и } D = NSCT^{-1}(R,K_R), K_D \neq K_R$$

Кроме упомянутых преобразований предлагаемая организация предполагает использование функции P(X) перестановки битов кода X ,через P^{-1} обозначая обратную перестановку, так, что:

$$X = P^{-1}(P(X))$$

При идентификации используется хеш-преобразование H(X), формирующая хеш-сигнатуру X. В качестве такой функции может быть использован один из хеш-алгоритмов, например, SHA.

Организация регистрации абонента схематично показана на рис.2.

При регистрации абонента A, им произвольно выбирается мнемонический пароль P_A, который вводится абонентом при каждом сеансе обращения к системе. При регистрации этот пароль P_A передается системе, где перемешивается с секретным постоянным кодом W:

$$K_A = P(P_A, W)$$

Полученный код K_A используется в качестве части ключа для преобразования универсального для всех абонентов системы секретного кода U во вторую часть пароля D_A абонента:

$$D_A = SCT(U, K_A)$$

Вычисленная описанным способом часть пароля D_A перемешивается:

$$D_{A'} = P(D_A)$$

возвращается системой абоненту вместе с его номером N_A. В памяти системы выделяется область памяти, адресуемая кодом N_A. В этой области записываются ключи доступа абонента А к ресурсам системы. Генерируется случайная строка S, которая сохраняется в области памяти абонента А. Эта строка вместе с D_A и N_A возвращаются абоненту А.

Обмен регистрационной информации производится в зашифрованном виде. Для этого абонент с использованием открытого ключа K_D системы шифрует мнемонический пароль P_A и случайно выбранный абонентом сеансовый ключ K_C : $T_1 = NSCT((P_A, K_C), K_D)$.

Система с использованием закрытого открывающего ключа K_R восстанавливает коды P_A и K_c. С использованием полученного сеансового

ключа K_C система шифрует сгенерированную часть D_A пароля абонента, его номер N_A и сохраненную строку S:

$$T_2 = SCT((D_A, N_A, S), K_C)$$

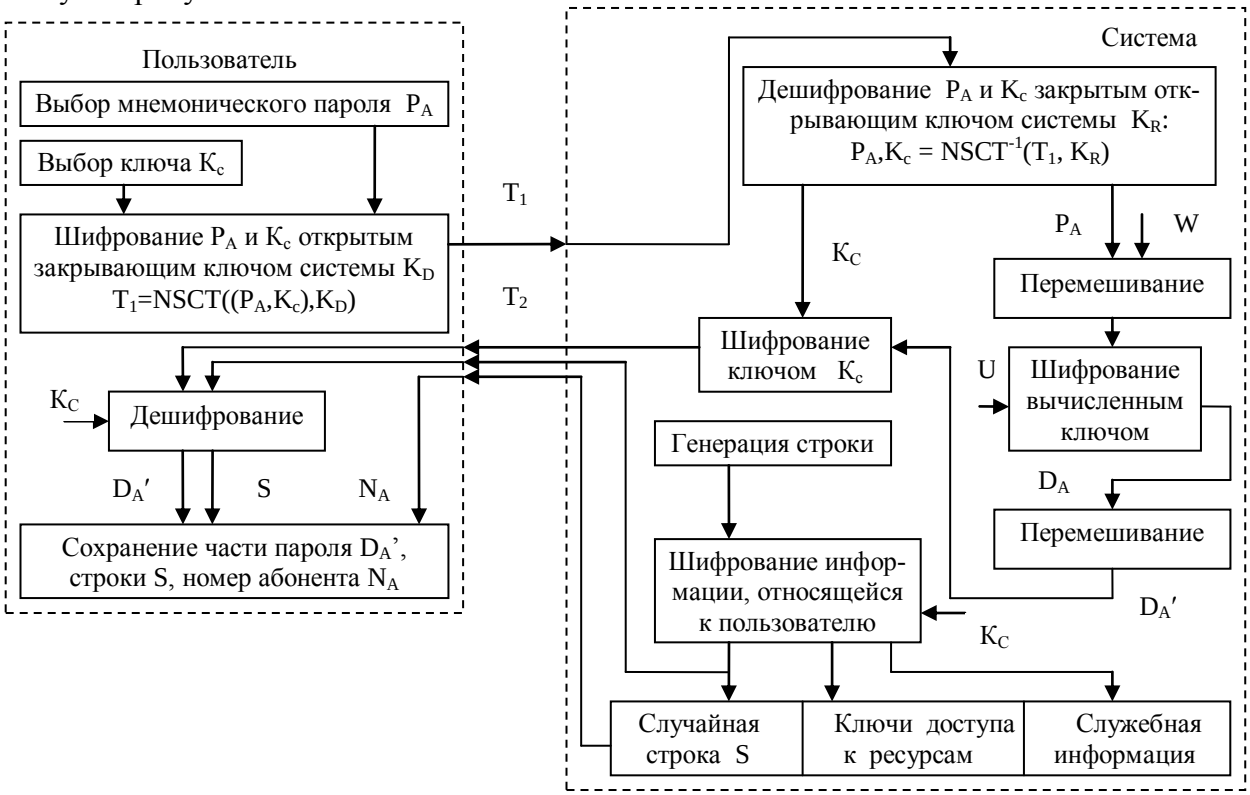

Рис.2. Структура операций, выполняемых при регистрации абонента

Таким образом, после регистрации в закрытой памяти системы сохраняются общие для всех абонентов коды W и U. Кроме того, в общей памяти системы в области, адресуемой N_A, сохраняется строка S и коды доступа к ресурсам.

Абонент сохраняет после регистрации в мнемонической памяти пароль P_A, в компьютере хранится часть пароля D_A и принятая от системы строка S.

Организация идентификации абонента при его обращении к системе схематично показана на рис.3.

При обращении абонента к системе, выполняется цикл его идентификации, включающий следующую последовательность действий:

1.Абонент А вводит строку мнемонического пароля P_A, который конкатенируется со строкой S. Над результатом конкатенации выполняется хеш-преобразование H с получением новой строки: $S' = H\langle P_A | S \rangle$

Строка S' замещает в памяти ранее хранившуюся строку S.

2.Абонентом выполняется конкатенация мнемонического пароля P_A, второй части пароля – D_A', номера N_A и строки S'. Результат конкатенации шифруется открытым закрывающим ключом K_D системы:

$$T = NSCT(P_A, D_{A'}, N_A, S')$$

Полученный код T отсылается в систему.

3.Многопользовательская система принимает идентифицирующий код T, посланный абонентом А и, используя свой секретный открывающий ключ K_R, выполняет дешифрацию компонент принятого кода:

$$P_A, D_{A'}, N_A, S' = NSCT^{-1}(T)$$

4.Обратной перестановкой битов система восстанавливает исходный код:

$$D_A = P^{-1}(D_{A'})$$

и вычисляет код ключа K_A путем перемешивания с секретным постоянным кодом W:

$$K_A = P(P_A, W)$$

5.С использованием полученного ключа K_A выполняется обратное криптографическое преобразование над кодом D_A:

$$R = SCT^{-1}(D_A, K_A)$$

Если результат равен коду U, то есть если R=U, то принимается решение о легальности абонента А. В противном случае, в доступе отказано.

6.Если установлен факт легальности абонента А, то выполняется идентификация прав

доступа абонента А к оговоренным ресурсам системы.

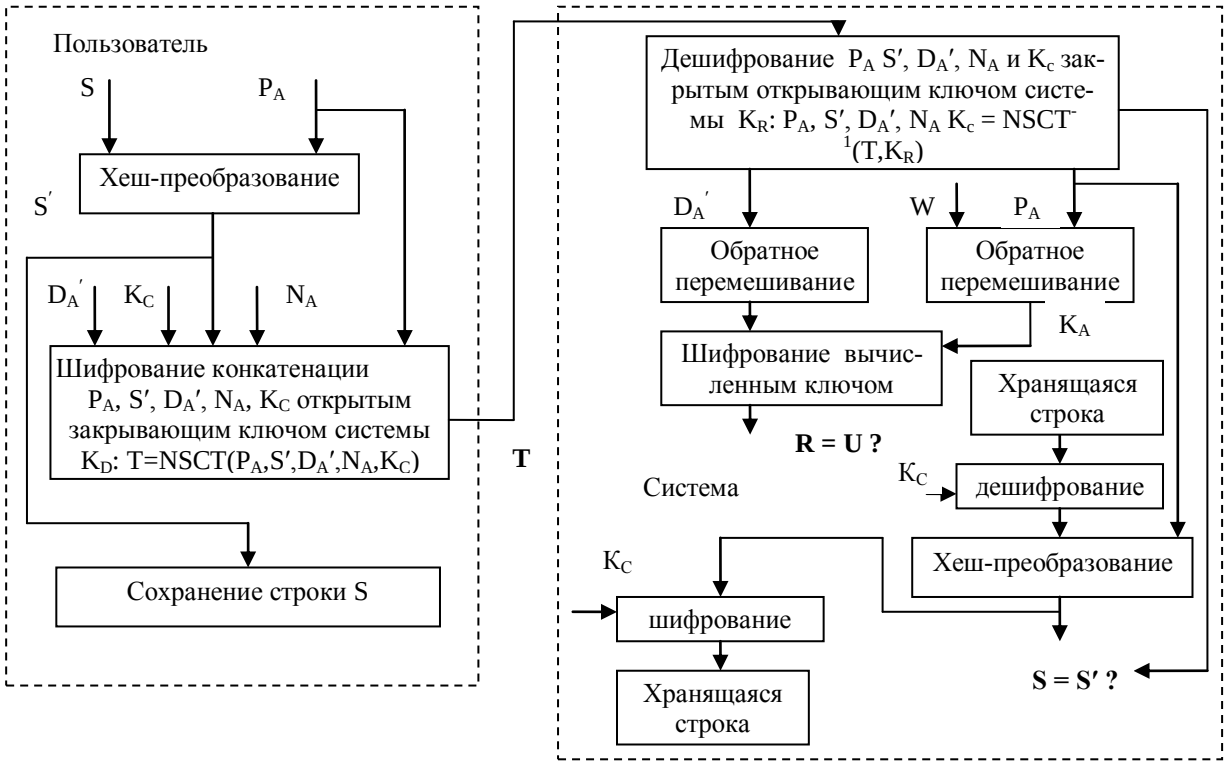

Рис.3. Структура цикла идентификации

Для этого из области памяти системы, адресуемой кодом N_A, считывается строка S_A.

Выполняется конкатенация полученного от абонента мнемонического пароля P_A со считанной из памяти строкой S_A. Над результатом конкатенации выполняется хеш-преобразование H с получением новой строки:

$$S_{A'} = H\langle P_A | S_A \rangle$$

Полученная в результате хеш-преобразования строка S_A' сравнивается со строкой S', полученной от абонента. Если эти строки совпадают, то есть если: $S_{A'} = S'$, то абоненту предоставляется право использовать ресурсы системы, обозначенные в области памяти N_A. В этом случае строка S' замещает в памяти ранее хранившуюся строку S_A в области памяти, адресуемой N_A. Если: $S_{A'} \neq S'$, то возникшая ситуация классифицируется как попытка доступа легального пользователя к ресурсам, доступ к которым не оговорен при его регистрации. Соответственно, в доступе отказано и замещения кода строки в области, адресуемой N_A, не производится.

Таким образом, предложенная организация реализует двухуровневую схему идентификации абонентов многопользовательских систем. На первом уровне со стороны системы используются только три секретных кода: открывающий ключ K_R, и произвольно выбираемые при инициализации системы коды W и U, одинаковые для всех абонентов. На первом уровне признаком того, что абонент легальный является совпадение результата описанного в пп.4-5 преобразования с секретным, единым для всех пользователей, кодом U, а не результатом совпадения с элементами списка идентификационной информации, как это реализовано в известных схемах идентификации удаленных пользователей [1,2]. Это обусловливает высокую скорость идентификации удаленных пользователей, причем, время идентификации не зависит от их количества. При этом многократно уменьшается объем хранящейся в системе секретной информации, что упрощает техническую реализацию закрытой памяти.

На втором уровне идентификация осуществляется сравнением строк, сгенерированных абонентом и системой. Это обеспечивает изменчивость идентифицирующей посылки для каждого из сеансов обращения к системе. Анализ отказов в доступе при реализации второго уровня идентификации позволяет эффективно выявлять попытки незаконного доступа к ресурсам системы и осуществлять мониторинг ее безопасности.

Предложенная организация идентификации использует только один цикл передачи идентифицирующей информации от абонента к системе. Это уменьшает риск незаконного проник-

новения в систему путем внедрения в процессе передачи. Кроме того, снижается использование важного для систем коллективного доступа ресурса – линии передачи.

Важным достоинством предложенной организации является то, что в ее рамках достигается разнесение информации, используемой при идентификации: выбранный абонентом мнемонический пароль P_A не сохраняется в компьютерной памяти, что исключает несанкционированный доступ к нему; однако подбор этого пароля неэффективен в силу того, что сам по себе он позволяет получить доступ к ресурсам системы. Дополнительная часть пароля D_A хранится в преобразованном виде D_A' только в компьютерной памяти абонента. Общая для всех абонентов часть пароля W хранится в закрытой памяти системы. Это не позволяет абоненту, которому не известны коды D_A и W, равно как и функция P перестановки, установить код U.

Для проникновения в систему нелегального пользователя, последний должен знать пароль P_A, соответствующий ему код D_A, номер N_A и код строки S. Разрядность D_A и P_A равна 256 (при использовании в качестве симметричного преобразования Rijndael), длина S больше 256. Очевидно, что успешный подбор указанных компонент маловероятен. Для получения доступа легального пользователя к недоступным для него ресурсам необходимо также подобрать связанные между собой необратимыми преобразованиями коды P_A, D_A, N_A и S. В случае проникновения к общей памяти системы можно получить коды строк S и номер области памяти, что не позволяет реализовать доступ извне: для этого надо подбирать коды P_A и D_A.

Выводы

Одним из наиболее эффективных подходов к снижению риска несанкционированного доступа к идентификационной информации со стороны системы целесообразно организовать хранения всех связанных с идентификацией данных в специальной энергонезависимой памяти, реализующей защиту на аппаратном уровне и, кроме того, реализующие все операции обработки таких данных.

Сформулированы принципы работы аппаратно защищенной памяти, ориентированной для использования в системах идентификации удаленных абонентов, обоснована и разработана структура такой памяти

Предложена двухуровневая организация идентификации абонентов многопользовательских систем, отличающаяся тем, что для снижения риска несанкционированного расширения прав доступа со стороны легальных абонентов, реализованы два уровня идентификации, на первом из которых выявляются легальные абоненты системы, а на втором – производится верификация их прав доступа. В отличии от известных схем идентификации, определение легальности абонента производится без обращения к области памяти, связанной с абонентом. Это позволяет ускорить идентификацию и сократить объем секретной информации до трех кодов: K_R, W и U, общих для всех абонентов, что упрощает реализацию специальной защищенной памяти.

Список литературы

1. Bengio S., Brassard G., Desmedt Y.G. Goutier C.,Quisquater J.J. “Secure implementation of identification system”, Jornal of Cryptology, v.4, n.3, 1991, pp.186-192.
2. Menezer A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC-Press, – 1997. – 780 p.
3. Bardis N.G., Polymenopoulos A., Bardis E.G., Markovskyy A.P. , “Methods for Increasing the Efficiency of the Remote User Authentication in Integrated Systems”, TRENDS IN COMPUTER SCIENCE, Volume 12. – No.1,– 2003. – pp.99-107.