УДК 004.056.52

Ю. В. Барышев, к. т. н.; В. А. Каплун; К. В. Неуймина

ДИСКРЕЦИОННАЯ МОДЕЛЬ И МЕТОД РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К РАСПРЕДЕЛЕННЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ

В работе представлен анализ моделей разграничения прав доступа. Предложена модель разграничения прав доступа, которая, используя особенности процесса хеширования, позволяет ограничить перечень рабочих станций, из которых пользователю разрешено получать удаленный доступ к информационным ресурсам. Обоснован выбор факторов аутентификации для рабочей станции и пользователя, что позволило разработать метод, который реализует разграничение прав доступа в соответствии с предложенной моделью.

***Ключевые слова**: аутентификация, хеширование, факторы аутентификации, модель разграничения прав доступа, параметры рабочей станции.*

Введение

Вследствие наличия многих возможных источников нарушения безопасности информации, обрабатываемой с использованием средств вычислительной техники, в частности персонала, злоумышленников, сбоев и т. д. [1], возникает задача обеспечения защищенности этой информации без существенного ухудшения показателей качества реализации процесса её обработки. Одним из методов защиты, используемых для решения этой задачи, является разграничение доступа пользователей компьютерной системы к имеющимся в системе информационным ресурсам [1, 2].

В условиях обработки информации с использованием рабочих станций предприятия, где работники службы защиты информации имеют возможность создать безопасные условия обработки информации, такой подход вполне достаточный. Однако с развитием мобильных вычислительных устройств и Интернета вещей (IoT) у легальных пользователей появилась возможность обрабатывать данные за пределами предприятия, в условиях, которые не способствуют сохранению конфиденциальности обрабатываемой информации. Соответственно возникла актуальная задача разработки таких модели и метода разграничения доступа, которые предотвращают обработку конфиденциальных данных с использованием незащищенных вычислительных средств.

Целью данного исследования является улучшение защиты конфиденциальной информации, предоставляемой пользователям с удаленных информационных ресурсов.

Для достижения цели необходимо решить следующие задачи:

– анализ известных моделей разграничения прав доступа;

– разработка модели разграничения прав доступа, обеспечивающей использование защищенных вычислительных средств для доступа к конфиденциальной информации;

– обоснование выбора факторов аутентификации пользователей для реализации данной модели;

– разработка метода разграничения прав доступа к распределенным информационным ресурсам на основе разработанной модели.

Анализ известных моделей разграничения прав доступа

Системы разграничения прав доступа осуществляют контроль над доступом субъектов информационной системы к объектам этой системы. В основе любой такой системы лежит модель разграничения прав доступа. Известные модели разграничения прав доступа делят на дискреционные, мандатные и ролевые [1, 3, 4].

Дискреционная модель разграничения прав доступа предусматривает, что права доступа

субъектов к каждому отдельному объекту системы могут быть ограничены на основе некоторого внешнего по отношению к системе правила [1, 3, 5].

Основным элементом дискреционного разграничения доступа является матрица доступа. Матрица доступа – матрица D размером $|S|\times|O|$, где S – множество субъектов информационной системы, а O – множество объектов этой системы. Элемент матрицы доступа $D[i,j]\subseteq R$ определяет права доступа i-го субъекта к j-му объекту (R – множество возможных прав доступа) [3 – 5].

Модель Харрисона – Руззо – Ульмана (модель HRU) является еще одним примером дискреционной модели разграничения прав доступа. Модель HRU предусматривает представление системы разграничения прав доступа конечным автоматом, который функционирует согласно определенным правилам перехода [3, 5].

Модель Take-Grant также является моделью дискреционного разграничения прав доступа и предоставляет возможность анализировать и проверять состояние безопасности информационной системы. В модели Take-Grant в качестве основных элементов используют граф доступа и преобразования над ним. Основной задачей модели является определение возможности получения прав доступа субъектом системы к объекту, состояние которого описано графом доступов. Формально описание модели Take-Grant выглядит следующим образом [3, 5, 6]:

– множество объектов – O, где $o_j \in O$, $O=\{o_1,o_2,...,o_j\}$, $j\in N$;

– множество субъектов – S, где $s_i \in S$, $S=\{s_1,s_2,...,s_i\}$, $i\in N$;

– множество активных субъектов – $S\subseteq O$;

– множество прав доступа R, где $r_n \in R$, $R=\{r_1,r_2,...,r_n\}\cup\{t,g\}$, где $t(take)$ – право брать права доступа, $g(grant)$ – права давать права доступа.

Используя данную модель, можно предположить состояния, в которых будет находиться информационная система в зависимости от разграничения прав доступа [5].

Преимуществом дискреционных моделей разграничения прав доступа является очевидность реализации системы разграничения доступа, универсальность и высокая гибкость. Однако ключевым недостатком является необходимость "ручного" администрирование этих систем, и следовательно, увеличение влияния человеческого фактора на надежность системы защиты информации, использующей такую модель разграничения прав доступа.

Мандатная модель сочетает защиту и ограничения прав, использующихся по отношению к компьютерным процессам, данным и системным устройствам, и предназначена для предотвращения их нежелательного использования [1 – 3, 5, 7].

Сегодня самым распространенным представителем мандатных моделей разграничения прав доступа является модель Белла – ЛаПадула [3, 5, 8]. Эта модель гарантирует, что субъект может ознакомиться с информацией только тогда, когда имеет на это достаточные полномочия, и любой субъект, кроме администратора, никоим образом не сможет осуществить перенос данных с объекта с высоким уровнем конфиденциальности в объект с более низким уровнем конфиденциальности. В модели Белла – ЛаПадула по грифам секретности распределяют объекты, имеющиеся в информационной системе, и по уровням секретности (мандатам) субъекты, действующие в этой системе. При этом необходимо обеспечение выполнения таких правил [3, 5]:

– субъекту заданного уровня секретности запрещено выполнять операцию "читать" для объектов более высокого уровня секретности (правило "no read up");

– субъекту заданного уровня секретности запрещено выполнять операцию "записывать" для более низкого уровня секретности (правило "no write down").

Если пользователь системы, который имеет высокий уровень допуска, запишет некоторые данные в объект с более низким уровнем секретности, то они могут стать доступными субъекту с более низким уровнем, чем разрешено политикой безопасности, уровнем допуска.

Основным недостатком данной модели является высокая сложность ее практической реализации средствами программирования, что порождает повышенные требования к ресурсам вычислительной системы при ее имплементации.

Ролевая модель (Role-Based Access Control – RBAC) предусматривает управление доступом как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям [3, 4, 8]. В этой модели компьютерная система представляется совокупностью таких множеств [3, 5, 7]: множества пользователей U; множества ролей R; множества полномочий P; множества сеансов C работы пользователей с системой.

Множество полномочий P в общем виде задают с помощью специальных механизмов, которые объединяют операции доступа и объекты доступа.

Преимуществом такой модели является то, что она требует меньших затрат времени на свое администрирование. Однако это преимущество приобретается за счет уменьшения гибкости модели разграничения прав доступа по сравнению с дискреционной. При этом ролевая модель более гибкая, чем мандатная, соответственно имеет выше потенциал адаптации к нуждам конкретной информационной системы. Таким образом, ролевую модель с практической точки зрения целесообразно рассматривать как компромиссный вариант между мандатной и дискреционной. Это обусловливает широкое использование ролевой модели, в частности в операционных системах и в системах управления базами данных [3 – 5, 9].

Таким образом, из выполненного анализа моделей разграничения доступа следует, что они имеют один общий недостаток – не обеспечивают ограничение рабочих станций, с которых пользователь имеет право получать доступ. Последний недостаток становится значимым в системах разграничения доступа к распределенным информационным ресурсам, в частности, файловых серверов и облачных сервисов. При организации доступа к распределенным информационным ресурсам необходимо, чтобы система разграничения доступа была максимально гибкой. Именно поэтому в рамках данного исследования целесообразно совершенствовать дискреционные модели разграничения прав доступа.

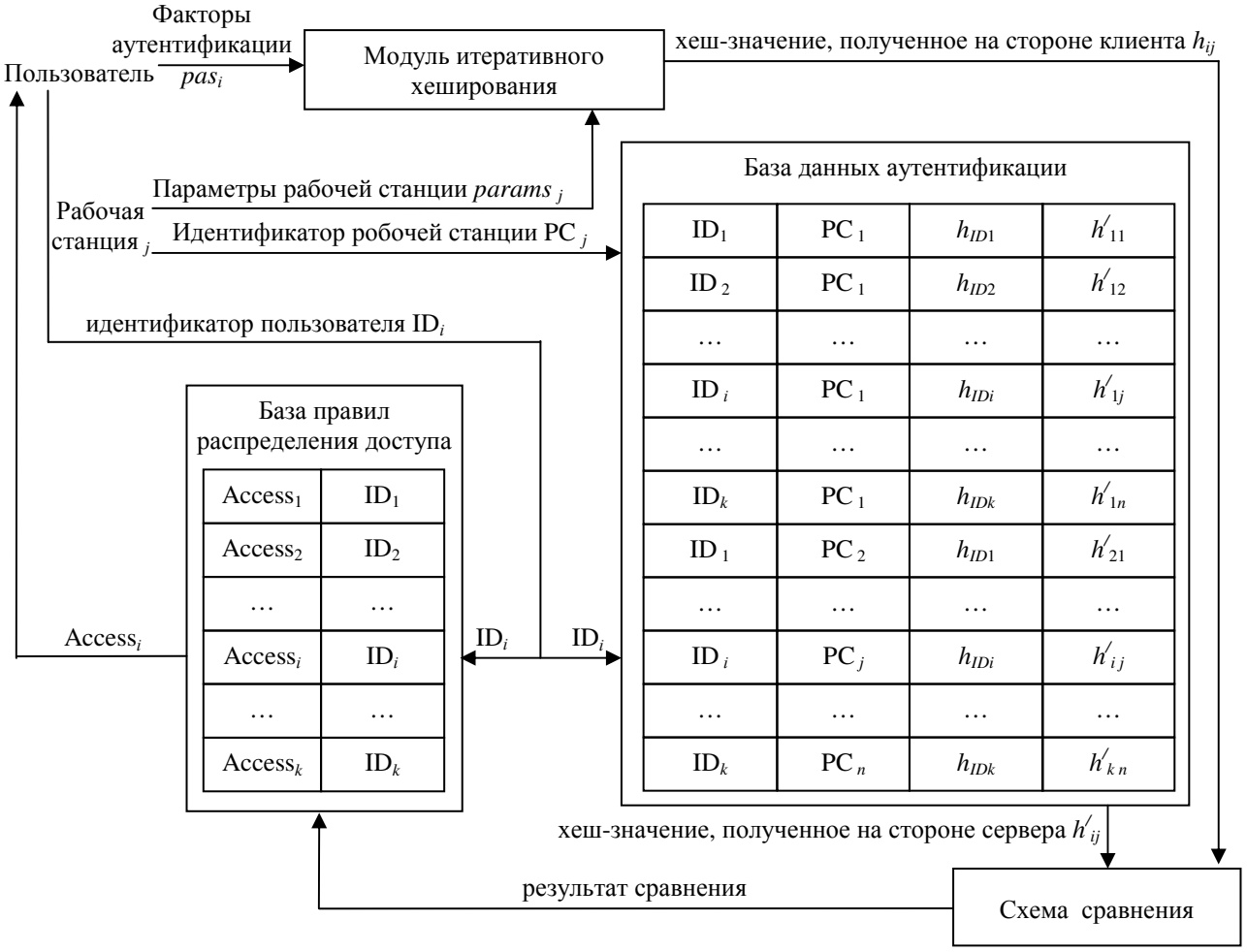
Модель разграничения прав доступа с привязкой к рабочим станциям

Подход к аутентификации пользователей, учитывающий рабочие станции, с которых инициируется эта аутентификация пользователя, может быть применен для разработки моделей разграничения прав доступа. В частности дискреционная модель на основе матрицы доступа при использовании предложенного подхода изменится следующим образом: вместо двухмерной матрицы в оригинальном подходе используют трехмерную матрицу $|S|\times|O|\times|PC|$, где PC – параметры рабочих станций (используемый субъектом инструментарий для получения доступа). Такая модель разграничения прав доступа требует специального метода аутентификации пользователей, поэтому предлагается для реализации подход к организации защищенного доступа пользователей к сетевым сервисам, рассмотрен в работах [10 – 12]. На рис. 1 изображена схема авторизации пользователя и рабочей станции [10].

Особенностью авторизации пользователей при такой модели разграничения прав доступа является то, что для защиты данных аутентификации должна использоваться итеративная конструкция хеширования. Например, к таким конструкциям относят конструкции Меркля – Дамгаарда, HAIFA и $MPH_q(2;1;1;1;0)$ [13, 14]. Конструкцию Меркля – Дамгаарда считают классической и формализуют следующим образом [13]:

$$h_i = f\left(m_i, h_{i-1}\right), \tag{1}$$

где h_i – промежуточное хеш-значение, полученное на i-м шаге; m_i – i-й блок данных; $f(\cdot)$ – функция сжатия, обеспечивающая фиксированную длину выходного значения.



ID_1	PC_1	h_{ID1}	h'_{11}
ID_2	PC_1	h_{ID2}	h'_{12}
…	…	…	…
ID_i	PC_1	h_{IDi}	h'_{1j}
…	…	…	…
ID_k	PC_1	h_{IDk}	h'_{1n}
ID_1	PC_2	h_{ID1}	h'_{21}
…	…	…	…
ID_i	PC_j	h_{IDi}	h'_{ij}
…	…	…	…
ID_k	PC_n	h_{IDk}	h'_{kn}

$Access_1$	ID_1
$Access_2$	ID_2
…	…
$Access_i$	ID_i
…	…
$Access_k$	ID_k

Рис. 1. Схема авторизации пользователя

Усовершенствованным вариантом конструкции Меркля – Дамгаарда, позволяющим повысить криптографическую стойкость к общим атакам за счет увеличения количества вычислений, является конструкция HAIFA [13]:

$$h_i = f\left(m_i, h_{i-1}, \#bits_i, r\right), \tag{2}$$

где $\#bits_i$ – количество уже захешированных битов сообщения; r – псевдослучайное число (криптографическая соль).

Поскольку дополнительные аргументы в функции сжатия в конструкции (2) по сравнению с конструкцией (1) приводят к увеличению нагрузки на сервер, который выполняет аутентификацию, предлагаем использовать хеш-функции, основанные на конструкциях многоканального хеширования $MPH_q\left(2;1;1;1;0\right)$ [14]:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, m_i, r_i^{(1)}, \#bits_i\right); \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, m_i, r_i^{(2)}, \#bits_i\right); \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, m_i, r_i^{(q)}, \#bits_i\right). \end{cases} \quad (3)$$

Ключевым свойством рассмотренных выше конструкций является то, что для хеширования $(i+1)$-го блока данных достаточно знать промежуточное хеш-значение h_i, независимо от того, каким образом оно было получено. Последнее делает возможным хранение на стороне сервера результата хеширования параметров факторов аутентификации i-го пользователя h_{IDi}, а не собственно значения этих параметров. Это обеспечивает выполнение такого равенства:

$$f\left(h_0, pas_i \,\|\, params_j\right) = f\left(f\left(h_0, pas_i\right), params_j\right), \quad (4)$$

где $h_{IDi} = f\left(h_0, pas_i\right)$.

Свойство, аналогичное (4), будут обеспечивать рассмотренные конструкции хеширования при дальнейшем увеличении длины сообщения, если это увеличение будет кратным длине блока данных m_i.

Для уменьшения нагрузки сервера предлагаем выполнять процесс хеширования параметров рабочих станций сразу после добавления соответствующего правила в базу данных аутентификации и хранения этого значения h_{ij} в базе, как это показано на рис. 1. За счет свойства хеширования, обусловленного использованием конструкций (1) – (3), происходит одновременно аутентификация и пользователя, и рабочей станции перед предоставлением доступа к информационному ресурсу.

Таким образом разделяют свойства субъекта, по которым происходит его аутентификация, на факторы, аутентифицирующие пользователя, и факторы, аутентифицирующие его вычислительные средства. Для разработки метода необходимо определить потенциальные факторы аутентификации.

Обоснование выбора факторов аутентификации

Методы аутентификации условно можно разделить на однофакторные и многофакторные [1, 2, 4, 15], где под факторами понимают свойство субъекта, по которому совершается его аутентификация. При этом однофакторные проще для реализации, однако обеспечивают ниже уровень безопасности, что обусловлено меньшей сложностью их подделки.

Парольная аутентификация является наиболее распространенным простым и привычным методом, в котором как фактор аутентификации используют знания пользователем определенного секретного слова – пароля [1, 4, 5, 15]. Использование данного фактора аутентификации не выдвигает дополнительные требования к аппаратной и программной части информационных ресурсов, однако часто оказывается неустойчивым вследствие значительного влияния человеческого фактора.

Известны методы аутентификации, которые предусматривают использование уникальных средств, обеспечивающих более стойкую защиту, чем парольная аутентификация. Такие факторы разделяют на две группы: пассивные, содержащие только информацию аутентификации, и активные, обладающие определенными вычислительными ресурсами и участвующими в реализации криптографических протоколов аутентификации [1, 4, 15].

Аутентификация при помощи уникальных средств имеет ряд недостатков: средство может быть похищено у пользователя, необходимо дополнительное аппаратное/программное обеспечение рабочих станций, возможна эмуляция действия фактора.

Биометрические методы аутентификации основываются на использовании оборудования

для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя [4, 15]. Такие средства позволяют с высокой точностью распознать владельца по конкретному биометрическому признаку, а подделать такие параметры сложнее по сравнению с рассмотренными выше. Существенным недостатком биометрической аутентификации является необходимость в дополнительном оборудовании каждой рабочей станции устройствами для получения биометрических характеристик.

Поскольку целью данного исследования является улучшение защиты конфиденциальности информации, предлагаем использовать многофакторную аутентификацию пользователей, основанную на знании им пароля и владении пассивным уникальным средством (флеш-носителем). Первый фактор позволяет уменьшить риск несанкционированного ознакомления с информацией в результате хищения носителя, а последний уменьшает влияние человеческого фактора.

Для аутентификации рабочей станции предлагаем использовать комбинацию из нескольких уникальных параметров этой станции. Факторы аутентификации рабочей станции используют такие характеристики компьютерной системы [15]: свойства программного обеспечения (системные файлы, версию операционной системы, дату создания и контрольную сумму BIOS, особенности файловой системы), свойства аппаратного обеспечения (производительность, серийные номера ключевых элементов аппаратного обеспечения, наличие дополнительной периферийной аппаратуры). Для данного исследования выбраны серийный номер жесткого диска, дата создания и контрольная сумма BIOS. Выбор этих факторов обусловлен их сравнительной устойчивостью и сложностью прогнозирования злоумышленником их значений.

В определенных случаях для предоставления уникальности каждому из сеансов аутентификации предлагаем к факторам аутентификации добавлять криптографическую соль – псевдослучайные числа [4, 13, 14]. Эта мера позволит избежать атаки повторной передачи захешированых факторов аутентификации и скрывать от злоумышленников, имеющих возможность анализировать трафик, как данные аутентификации пользователя, так и рабочую станцию, с которой он работает.

Метод разграничения прав доступа к распределенным информационным ресурсам

Для реализации метода предлагаем структуру программного средства клиент-серверной архитектуры. В соответствии с методом разграничения прав доступа на стороне клиента выполняют следующие действия:

– с помощью модуля определения факторов аутентификации пользователя он вводит свои учетные данные и происходит определение параметров факторов авторизации (например, пароля и параметров флэш-носителя);

– одновременно происходит определение параметров факторов аутентификации рабочей станции (для задач данного исследования – серийного номера жесткого диска, даты создания и контрольной суммы BIOS);

– с помощью модуля итеративного хеширования на стороне клиента определяют хеш-значения от результата конкатенации значений параметров факторов аутентификации пользователя и рабочей станции, а также криптографической соли:

$$h_{ij} = f\left(h_0,\ pas_i \parallel params_j \parallel r\right); \tag{5}$$

– полученный результат хеширования, идентификатор рабочей станции и учетную запись пользователя направляют на сторону сервера.

На рис. 2 приведена структура клиентского приложения для реализации метода.

Для реализации метода на стороне сервера происходят такие действия:

– по полученным от клиента значениям учетной записи пользователя и идентификатора

рабочей станции определяют хеш-значение факторов аутентификации пользователя и параметры рабочей станции;

– происходит хеширование параметров рабочей станции и криптографической соли:

$$h'_{ij} = f\left(h_i, params_j \| r\right); \quad (6)$$

– на основе сравнения вычисленного и полученного хеш-значений принимают решение о разрешении или запрете доступа пользователя.

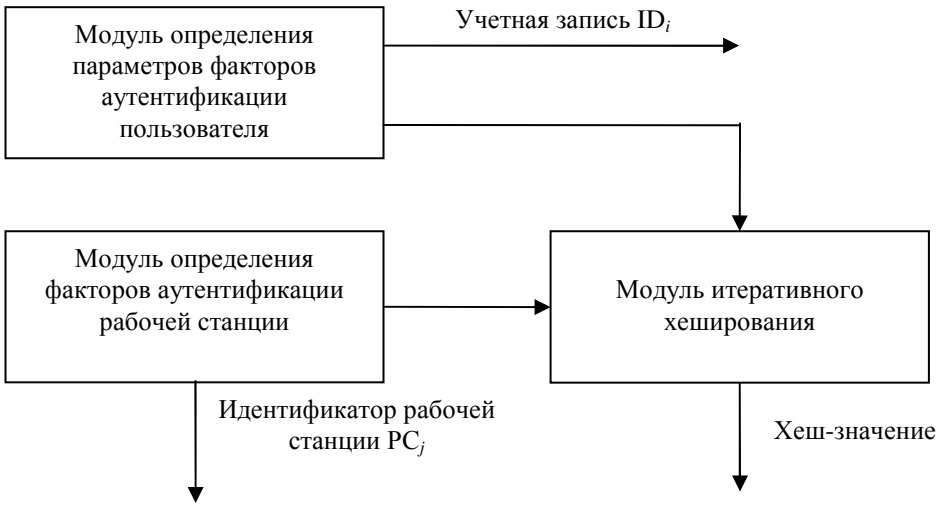


Рис. 2. Структура клиентского приложения для реализации метода

На рис. 3 приведена структура серверного приложения, взаимодействующего с клиентским приложением.

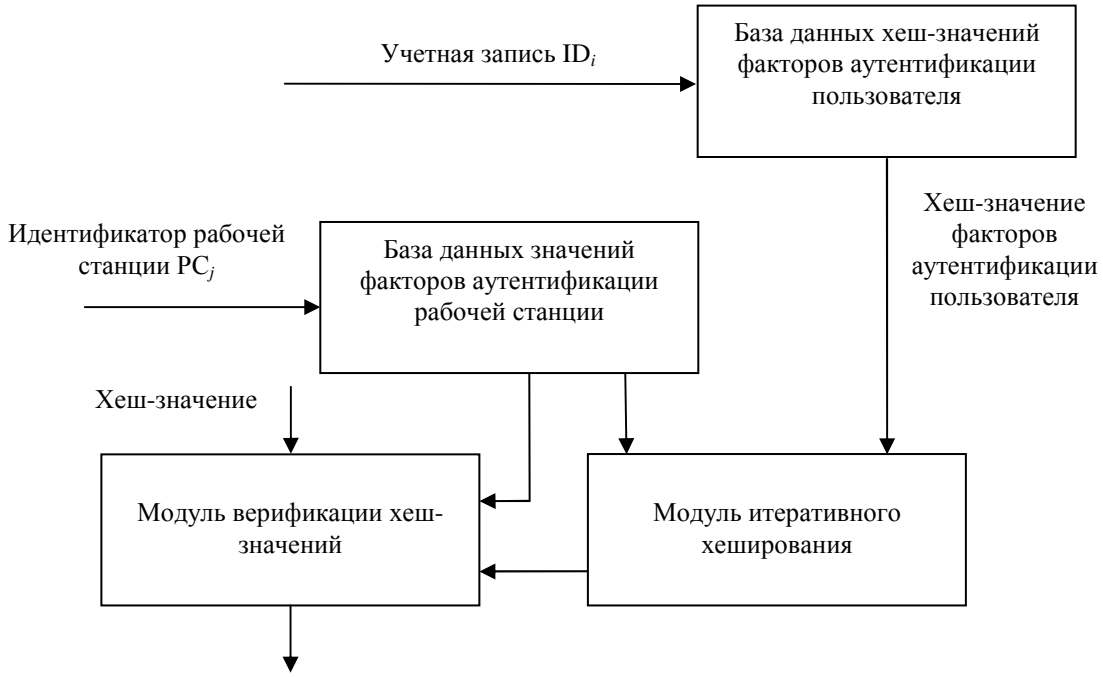


Рис. 3. Структура серверного приложения для реализации метода

Предложенный метод может модифицировать путем предварительного вычисления хеш-

значений для всех комбинаций {пользователь; рабочая станция}. Это позволит уменьшить загруженность сервера, однако сделает нецелесообразным использование криптографической соли, что уменьшит устойчивость метода ко взлому.

Выводы

Выполненный анализ моделей разграничения прав доступа выявил их нацеленность на аутентификацию пользователя. При этом данные модели не учитывают рабочую станцию, с которой авторизованный пользователь пытается получить доступ. При развитии мобильных вычислительных средств и IoT этот недостаток порождает уязвимость обрабатываемой информации, поскольку исчезают гарантии, что рабочая станция на стороне клиента имеет адекватную систему защиты информации. Для устранения этого недостатка предлагаем модель разграничения прав доступа, которая предусматривает как ограничение пользователей, так и ограничение рабочих станций, с которых пользователь может получить информацию. При этом перечень рабочих станций предлагаем ограничивать для каждого пользователя. Такая модель не только позволяет обеспечить соответствующий уровень защиты информации при ее обработке пользователями, но и уменьшить уязвимость системы к атакам инсайдеров, ведь каждый работник привязан к своему рабочему месту, что уменьшает его возможности незаметной реализации атаки.

Предложены факторы авторизации пользователей и рабочей станции для реализации этой модели. Разработана структура средств разграничения прав доступа, что позволяет предложить метод, который реализует разграничение прав доступа в соответствии с моделью. Особенностью метода является использование итеративного хеширования, которое позволяет без сохранения ключей хеширования и факторов аутентификации пользователя на стороне сервера выполнять одновременную проверку подлинности и их, и рабочих станций.

СПИСОК ЛИТЕРАТУРЫ

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.

2. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. – М. : Горячая линия-Телеком, 2004. – 280 с.

3. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Издательский центр "Академия", 2005. – 144 с.

4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / [А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.] ; под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия-Телеком, 2009. – 552 с.

5. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Краткий курс / В. Л. Цирлов. – М. : Изд-во Феникс, 2008. – 174 с.

6. Миронова В. Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В. Г. Миронова, А. А. Шелупанов, Н. Т. Югов // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 206 – 210.

7. Теория и практика обеспечения информационной безопасности / [под ред. П. Д. Зегжды]. – М : Яхтсмен, 1996. – 302 с.

8. Жора В. В. Підхід до моделювання рольової політики безпеки / В. В. Жора // Правове нормативне та метрологічне забезпечення систем захисту інформації в Україні : інтернет журн. – 2003. – № 7. – С. 45 – 49.

9. Панасенко С. Методы аутентификации / С. Панасенко // Банки и технологии. – 2002 – № 3. – С. 56 – 60.

10. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун // Інформаційні технологій та комп'ютерна інженерія. – 2014. – № 2. – С. 13 – 17.

11. Баришев Ю. В. Метод авторизації віддалених користувачів / Ю. В. Баришев, К. В. Неуйміна // Тези доповідей П'ятої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації" м. Вінниця, 19-21 квітня 2016 року. – Вінниця : ВНТУ, 2016. – С. 65 – 67.

12. Баришев Ю. В. Метод та засіб автентифікації користувачів файлового серверу / Ю. В. Баришев, К. І. Кривешко // Праці IV Міжнародної науково-практичної конференції "Обробка сигналів і негауссівських процесів", присвяченої пам'яті професора Ю. П. Кунченка : Тези доповідей. – Черкаси : ЧДТУ, 2013. – С. 109 – 111.

13. Biham E. A Framework for Iterative Hash Functions: HAIFA [Електронний ресурс] / Eli Biham, Orr Dunkelman // Second cryptographic hash workshop. – 2006. – 9 с. – Режим доступу до ресурсу : http://csrc.nist.gov/groups/ST/hash/documents/DUNKELMAN_NIST3.pdf.

14. Баришев Ю. В. Методи та засоби швидкого багатоканального хешування даних в комп'ютерних системах. автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.05 «Комп'ютерні системи та компоненти» / Ю. В. Баришев. – Вінниця : ВНТУ, 2012. – 20 с.

15. Дудатьєв А. В. Захист програмного забезпечення. Частина 1. Навчальний посібник / А. В. Дудатьєв, В. А. Каплун, С. П. Семеренко. – Вінниця : ВНТУ, 2005. – 140 с.

Барышев Юрий Владимирович — к. т. н., доцент кафедры защиты информации, e-mail: yuriy.baryshev@gmail.com.

Каплун Валентина Аполинарьевна – старший преподаватель кафедры защиты информации.

Неуймина Кристина Владимировна — студентка кафедры защиты информации, e-mail: kris.vladimirovna99@gmail.com.

Винницкий национальный технический университет.