УДК 004.421.2:511.344

А. В. Курилец[1], **В. В. Смелов**[1], **Н. Горанин**[2]
[1]Белорусский государственный технологический университет
[2]Вильнюсский технический университет имени Гедеминаса

МЕТОД АВТОРИЗАЦИИ НА ОСНОВЕ РАЗЛОЖЕНИЯ ЧИСЕЛ НА ПРОСТЫЕ СОМНОЖИТЕЛИ

Статья посвящена описанию метода авторизации на основе разложения чисел на простые сомножители. В ней представлено формальное описание системы авторизации, включающей субъекты и объекты авторизации, а также алгоритмы процедуры авторизации. Предлагаемая система авторизации предусматривает единственный тип привилегии, который описывает взаимоотношения между субъектами и объектами системы и может интерпретироваться в бинарной форме: доступен / не доступен или разрешен / запрещен. Вводится понятие составных объектов, доступ к которым обусловливается разрешением доступа к другим объектам авторизации. Рассматривается принцип построения иерархии объектов авторизации. Вводится понятие роли как поименованного набора привилегий, описывается алгоритм процедуры назначения роли субъекту авторизации. Описание системы авторизации сопровождается примерами, поясняющими принципы ее работы, а также оценками, обозначающими границы ее применения.

Ключевые слова: информационная безопасность, авторизация, система авторизации, субъект авторизации, объект авторизации, привилегия, роль.

Для цитирования: Курилец А. В., Смелов В. В., Горанин Н. Метод авторизации на основе разложения чисел на простые сомножители // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2021. № 1 (242). С. 43–47.

A. V. Kurylets[1], **V. V. Smelov**[1], **N. Goranin**[2]
[1]Belarusian State Technological University
[2]Vilnius Gediminas Technical University

AUTHORIZATION METHOD BASED ON THE DECOMPOSITION OF NUMBERS INTO SIMPLE MULTIPLIERS

The article is devoted to the description of the authorization method based on the decomposition of numbers into simple somno-residents. The article presents a formal description of the authorization system, which includes subjects and objects of authorization, as well as algorithms for the authorization procedure. The proposed authorization system provides for a single type of privilege that describes the relationship between the subjects and objects of the system and can be interpreted in binary form: available / not available or allowed/denied. The concept of composite objects is introduced, access to which is determined by the permission of access to other authorization objects. The principle of constructing a hierarchy of authorization objects is considered. The concept of a role as a named set of privileges is introduced, an algorithm for assigning a role to an authorization subject is described. The description of the authorization system is accompanied by examples that explain the principles of its operation, as well as assessments indicating the boundaries of its application.

Key words: information security, authorization, authorization system, authorization subject, authorization object, privilege, role.

For citation: Kurylets A. V., Smelov V. V., Goranin N. Authorization method based on the decomposition of numbers into simple multipliers. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2021, no. 1 (242), pp. 43–47 (In Russian).

Введение. Построение системы информационной безопасности начинается с выявления (идентификации) субъектов и объектов информационной безопасности. В информационных системах под субъектами подразумеваются активные компоненты (пользователи, программные средства), а под объектами – пассивные компоненты системы (аппаратное обеспечение, информационные ресурсы, каналы связи, программные коды). При этом все процессы, происходящие в информационной системе, с точки зрения информационной безопасности сводятся к взаимоотношению между субъектами и объектами, причем в некоторых случаях субъекты могут выступать в качестве объектов информационной безопасности и наоборот.

Взаимоотношение между субъектами и объектами регламентируется правилами, которые являются воплощением политики информационной безопасности информационной системы. Реализация правил обычно сводится к двум процедурам: аутентификации и авторизации.

Процедура аутентификации реализует алгоритм, который позволяет определить правомочность внешней по отношению к информационной системе сущности выполнять действия в информационной системе от имени ее субъекта. В простейшем случае в качестве сущности может выступать пользователь информационной системы, в качестве процедуры аутентификации – проверка имени и пароля, а субъект в этом случае – это регистрационная запись пользователя в системе.

Процедура авторизации реализует алгоритм проверки действий субъектов по отношению к объектам на соответствие правилам, воплощающим политику безопасности информационной системы. Элементарное действие, которое может быть разрешено или отменено, обычно называют привилегией. Проверка, как правило, сводится к сравнению формального описания (дескриптора) объекта с формальным описанием (дескриптором) субъекта.

Ниже рассматривается система авторизации, реализующая мандатную модель доступа [1] и основанная на представлении дескрипторов субъектов и объектов информационной безопасности в виде произведений простых сомножителей и предусматривающая единственный тип привилегии – доступ субъекта к объекту.

Основная часть. В общем случае формальное описание системы S авторизации произвольной информационной системы может быть описано в виде тройки

$$S = <R, U, A>,$$

где $R = \{r_1, r_2, r_3, ..., r_N\}$ – конечное множество объектов (ресурсов) информационной системы, доступ к которым регулируется системой авторизации S;

$U = \{u_1, u_2, u_3, ..., u_L\}$ – конечное множество субъектов информационной системы, доступ которых к объектам R регулируется системой авторизации S;

$A \subset U \times R$ – бинарное отношение, определенное на декартовом произведении $U \times R$ и такое, что если $< u, r > \in A$, то субъекту $u \in U$ разрешен доступ (привилегия) к объекту $r \in R$.

Бинарное отношение A может быть представлено в виде графа $G_A = < U \cup R, A >$, где $U \cup R$ – множество вершин графа; A – множество дуг. На рис. 1 изображен пример графа G_A. Вершинам графа соответствуют субъекты $\{ u_1, u_2, u_3 \}$ и объекты $\{r_1, r_2, r_3, r_4\}$, а дугам – элементы отношения A. Например, дуга $< u_1, r_2 >$ описывает возможность доступа субъекта u_1 к объекту r_2, дуги, входящие в вершину r_1, описывают возможность доступа всех субъектов к объекту r_1, а изолированная вершина r_4 соответствует объекту, недоступному для всех субъектов.

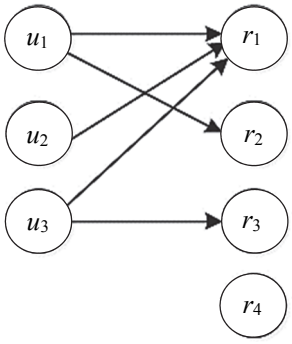

Рис. 1. Граф $G_A = < U \cup R, A >$

По всей видимости, построение бинарного отношения A над множеством $U \times R$ можно свести к построению характеристической функции

$$H(u, r) = \begin{cases} 1, & < u, r > \in A, \\ 0, & < u, r > \notin A, \end{cases}$$

т. е. субъекту $u \in U$ разрешен доступ к объекту $r \in R$, если $H(u, r) = 1$. Тогда бинарное отношение A может быть записано в виде $A = \{< u, r > \in A \mid H(u, r) = 1\}$.

Рассмотрим систему авторизации S, построенную на следующем известном свойстве натуральных чисел.

Пусть $n \in \mathbf{N}$ натуральное число. Тогда верно следующее утверждение: $\forall n \in \mathbf{N} \wedge n > 1 : n = p_1^{\alpha} p_2^{\alpha} ... p_m^{\alpha}$, где p_i – простые, а α_i, $i = \overline{1, m}$ – натуральные числа. Другими словами, любое натуральное число, превышающее единицу, может быть представлено в виде произведения простых чисел. Причем такое разложение является единственным [2]. Например, $65\,340 = 2^2 \times 3^3 \times 5 \times 11^2$.

Пусть $P = \{p_1, p_2, p_3, ..., p_N\}$ – конечное множество простых чисел. Представим множество R объектов авторизации в виде множества пар $R = \{r_i = < \dot{r}_i, \ddot{r}_i >, i = \overline{1, N}\}$, где $\dot{r}_i$ – идентификатор объекта, а $\ddot{r}_i$ – его дескриптор. Значение идентификатора может быть выбрано произвольно при условии его уникальности, а значение дескриптора $\ddot{r} = p_i$, $p_i \in P$, $i = \overline{1, N}$ – простое число.

Множество U субъектов информационной системы тоже представим в виде множества пар $U = \{ u_j = < \dot{u}_j, \ddot{u}_j >, j = \overline{1, L} \}$, где $\dot{u}_j$ – идентификатор субъекта, а $\ddot{u}_j$ – дескриптор. Как и прежде, значение идентификатора может быть выбрано произвольно при условии его уникальности, а дескриптор субъекта зададим в виде произведения:

$$\ddot{u}_j = x_1 x_2 x_3 ... x_N,$$

где $x_i = \begin{cases} 1, & < u_j,\ r_i > \notin A, \\ \ddot{r}_i, & < u_j,\ r_i > \in A. \end{cases}$

Другими словами, $\ddot{u}_j$ является произведением дескрипторов $\ddot{r}_i$ тех объектов системы S, доступ к которым разрешен субъекту u_j.

Характеристическая функция H проверки принадлежности пары $< u_j, r_j >,\ j = \overline{1, L},\ i = \overline{1, N}$ множеству A может быть записана в следующем виде:

$$H\left(u_j,\ r_i\right) = \begin{cases} 1, & \ddot{u}_j \bmod \ddot{r}_i = 0, \\ 0, & \ddot{u}_j \bmod r_i \neq 0. \end{cases}$$

Рассмотрим пример системы авторизации $S = < R, U, A >$, включающую пять объектов $R = \{< 1,3 >, < 2,5 >, < 3,7 >, < 4,11 >, < 5,13 >\}$ и три субъекта $U = \{< 1, \ddot{u}_1 >, < 2, \ddot{u}_2 >, < 3, \ddot{u}_3 >\}$. Пусть отношение A описывается следующей таблицей.

R	$< 1, \ddot{u}_1 >$	$< 2, \ddot{u}_2 >$	$< 3, \ddot{u}_3 >$
<1,3>	+	+	
<2,5>	+	+	
<3,7>	+	+	+
<4,11>	+		+
<5,13>	+		+

Строки таблицы соответствуют объектам с заданными дескрипторами, столбцы – субъектам системы авторизации S. На пересечении строки i и столбца j стоит плюс, если $< u_j,\ r_i > \in A$ или, другими словами, субъекту u_j разрешен доступ к объекту r_i. Тогда дескрипторы авторизации $\ddot{u}_j$ субъектов примут следующие значения:

$$\ddot{u}_1 = 3 \times 5 \times 7 \times 11 \times 13 = 15\,015,$$

$$\ddot{u}_1 = 3 \times 5 \times 7 = 105,$$

$$\ddot{u}_1 = 7 \times 11 \times 13 = 1001.$$

Значения выражения $\ddot{u}_j \bmod \ddot{r}_i$, вычисляемого в характеристической функции H, представим в табличной форме.

R	<1,15015>	<2,105>	<3,1001>
<1,3>	0	0	2
<2,5>	0	0	1
<3,7>	0	0	0
<4,11>	0	6	0
<5,13>	0	1	0

Очевидно, что характеристическая функция H будет принимать значение 1, если субъекту разрешен доступ к объекту и 0 в другом случае.

В некоторых случаях объекты системы авторизации могут иметь более сложную схему доступа. Например, пусть r_1, r_2, r_3 – три объекта системы авторизации S. При этом в системе должен быть обеспечен независимый авторизированный доступ к каждому из объектов r_1 и r_2, а к объекту r_3 разрешен доступ только тем субъектам, которым разрешен доступ и к r_1 и к r_2. Такая зависимость авторизированного доступа может быть разрешена, если выбрать в качестве дескриптора объекта r_3 приведенное произведение дескрипторов объектов r_1 и r_2: $\ddot{r}_3 = \ddot{r}_1\ddot{r}_2 \,/\, / \gcd\left(\ddot{r}_1,\ \ddot{r}_2\right)$, где gcd – функция, вычисляющая наибольший общий делитель для двух натуральных чисел. Очевидно, что верно следующее общее утверждение:

$$\forall u_j \in U,\ \left\{r_{i_1},\ r_{i_2},\ r_{i_3} = < \dot{r}_{i_3},\ \ddot{r}_{i_1}\ddot{r}_{i_2} \,/ \right.$$

$$\left. / \gcd\left(\ddot{r}_{i_1},\ \ddot{r}_{i_2}\right) >\right\} \subset R \mid H\left(u_j,\ r_{j_1}\right) =$$

$$= H\left(u_j,\ r_{j_2}\right) = 1 : H\left(u_j,\ r_{j_3}\right) = 1.$$

Другими словами, для рассматриваемого примера, если дескриптор объекта r_3 равен приведенному произведению дескрипторов объектов r_1 и r_2 $\left(\ddot{r}_3 = \ddot{r}_1\ddot{r}_2\right) / \gcd\left(\ddot{r}_1,\ \ddot{r}_2\right)\big)$, то субъект авторизации, имеющий доступ к объектам r_1 и r_2, имеет доступ и к объекту r_3. Далее, объекты, доступ к которым обусловлен доступом к другим объектам, будем называть составными объектами, а объекты, доступ к которым не зависит от доступа к другим объектам, – элементарными объектами авторизации. При этом будем говорить, что составные объекты составлены из других объектов.

Обобщив понятие составного объекта, можно строить иерархические системы объектов авторизации. На рис. 2 приведен пример ориентированного графа, описывающего иерархическую систему объектов авторизации: вершины графа соответствуют объектам авторизации, а ребра – зависимостям между ними.

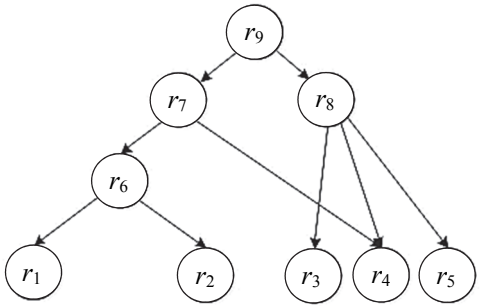

Рис. 2. Иерархическая система объектов авторизации

Система объектов, представленная на рис. 2, содержит пять элементарных r_1, r_2, r_3, r_4, r_5, четыре составных объекта авторизации r_6, r_7, r_8, r_9. Следует обратить внимание на то, что объекты r_7, r_9 составлены из составных объектов, а r_6 и r_8 – из элементарных.

Пусть, например, $r_1 = < 1,3 >$, $r_2 = < 2,5 >$, $r_3 = < 3,7 >$, $r_4 = < 4,11 >$, $r_5 = < 5,13 >$ – элементарные объекты авторизации, представленные на рис. 2. Тогда составные объекты будут выглядеть следующим образом:

$$r_6 = < 6, \frac{3 \times 5}{\gcd(3,5)} > = < 6,15 >,$$

$$r_7 = < 7, \frac{15 \times 11}{\gcd(15,11)} > = < 7,165 >,$$

$$r_8 = < 8, \frac{7 \times 11 \times 13}{\gcd(7,11)\gcd(77,13)} > = < 8,1001 >,$$

$$r_9 = < 9, \frac{165 \times 1001}{\gcd(165,1001)} > = < 9,15015 >.$$

В системах авторизации информационных систем используется понятие роли. Обычно роль – это поименованный (используется уникальный идентификатор) набор привилегий (в нашем случае привилегия – возможность доступа к объектам авторизации). Роль может быть назначена субъектам авторизации, в результате чего субъекты приобретают (наследуют) привилегии (возможности доступа), которыми обладала эта роль. При этом одному субъекту может быть назначено несколько ролей, а одна роль может быть назначена нескольким субъектам.

Пусть $T = \{t_1, t_2, t_3, \ldots, t_M\}$ – множество ролей, заданных в системе авторизации S. По аналогии с субъектами, роль можно представить как множество пар $T = \left\{ \left\langle \dot{t}_k, \ddot{t}_k \right\rangle, \ k = 1, M \right\}$, где $\dot{t}_k$ – идентификатор роли, выбранный из условия уникальности, а $\ddot{t}_k$ – дескриптор.

Назначение роли t_k к субъекту u_j будем обозначать с помощью оператора grant и записывать в следующей форме: $t_k grant u_j$. Формально определим оператор grant следующим образом:

$$\forall u_j \in U, \ < \dot{u}_J, \ \ddot{u}_j > \in U, \ t_k \in T : t_k \ grant \ u_j \Leftrightarrow u_j = \left\langle \ddot{u}_J, \ \ddot{u}_j \ddot{t}_k \ / \gcd\left(\ddot{u}_j, \ \ddot{t}_k\right) \right\rangle.$$

Дескриптор роли зададим в виде произведения:

$$\ddot{t}_k = x_1 x_2 x_3 \ldots x_N,$$

где $x_i = \begin{cases} 1, \ \forall u_j \in U \mid t_k grant \, u_j : \left\langle u_j, r_i \right\rangle \notin A, \\ \ddot{r}_i, \ \forall u_j \in U \mid t_k grant \, u_j : \left\langle u_j, r_i \right\rangle \in A. \end{cases}$

Другими словами, $\ddot{t}_k$ является произведением дескрипторов $\ddot{r}$ тех объектов системы S, доступ к которым может обеспечиваться назначением роли t_k любому субъекту.

Продолжим пример, рассмотренный выше: $R = \{< 1,3 >, < 2,5 >, < 3,7 >, < 4,11 >, < 5,13 >\}$ – множество объектов; $U = \{< 0,15015 >, < 2,105 >, < 3,1001 >\}$ – множество субъектов авторизации.

Пусть $t = \left\langle A, \ \ddot{t} \right\rangle$ – набор привилегий доступа к объектам системы авторизации, которой задается с помощью следующей таблицы:

R	$\left\langle A, \ \ddot{t} \right\rangle$
<1,3>	
<2,5>	+
<3,7>	
<4,11>	
<5,13>	+

Таблица состоит из пяти строк, соответствующих объектам авторизации, $r_i \in R$, $i = \overline{1,5}$, и единственного столбца, соответствующего роли с идентификатором A. При этом в строке i стоит плюс, если применение (*grant*) роли $\left\langle A, \ \ddot{t} \right\rangle$ к произвольному субъекту $u \in U$ приводит к изменению значения дескриптора $\ddot{u}$ этого субъекта, разрешающему доступ субъекта u к соответствующему объекту $r_i \in R$. Очевидно, что $\ddot{t} = 5 \times 13 = 65$.

Применение роли $<A, 65>$ субъектам $< 1,15015 >$, $< 2,105 >$, $< 3,1001 >$ приведет к следующим изменения их дескрипторов:

$$<A, 65> grant < 1,15015 > \Leftrightarrow u_1 = < 1,15015 >;$$

$$<A, 65> grant < 2,105 > \Leftrightarrow u_2 = < 2,1365 >;$$

$$<A, 65> grant < 3,1001 > \Leftrightarrow u_3 = < 3,5005 >.$$

Заметим, что дескриптор субъекта u_1 не претерпел изменения после применения роли $< A, 65 >$, так как роль предоставила привилегии доступа к объектам $< 2,5 >$ и $< 5,13 >$, доступ к которым у субъекта u_1 уже был. Дескрипторы субъектов u_2 и u_3 изменились – они приобрели дополнительные привилегии доступа: субъект u_2 к объекту $< 5,13 >$, а субъект u_3 к объекту $< 2,5 >$.

Заключение. Применение традиционных подходов авторизации, как правило, приводит к необходимости хранения дескрипторов авторизации на внешнем носителе, извлечении их и сверки при каждой операции, выполняемой субъектом информационной безопасности. При большой интенсивности операций прибегают к кэшированию дескрипторов, чтобы снизить затраты на процедуру проверки правомочности выполнения запрашиваемой операции. При этом обычно дескриптор авторизации применяется в форме списка ACL [3], каждый элемент которого в общем случае содержат информацию о субъекте, объекте и разрешенной (или запрещенной) привилегии. С другой стороны, разработчикам информационных систем часто приходится сталкиваться с необходимостью разработки простых приложений, доступ к небольшой функциональности которых регулируется простым правилом: доступен или не доступен. Характерным примером такого приложения может служить

микросервис [4], который по определению должен быть простым в использовании и разработке.

Основным достоинством предложенной системы авторизации является простота ее реализации, так как в основе лежат простейшие арифметические операции.

Основной недостаток – ограниченность применения, связанная с размерностью данных современных компьютеров. Дескрипторы (произведение разных простых чисел), описывающие объекты и привилегии доступа к ним субъектов информационной безопасности, представляют собой беззнаковые положительные числа, размерность которых в современных компьютерах не превышает 64 бита. Такое ограничение приводит к тому, что максимальное количество элементарных объектов в предлагаемой системе не может превышать 15. Даже если размерность данных возрастет до 128 бит, это ограничение сдвигается лишь до 26. Применение вычисления с применением алгоритмов «длинной арифметики» усложняет программную реализацию и, главное, значительно увеличивают процедуру авторизации, основанную на операции деления – наиболее трудоемкой операции в «длинных» вычислениях.

Применение предложенного метода авторизации для такого рода программных приложений, по мнению авторов, является целесообразным: программная реализация является простой, проверка правомочности доступа не требует больших вычислительных ресурсов, предлагаемая процедура авторизации просто встраивается в существующие сетевые протоколы (например, протокол RFC 7519 для создания токенов доступа, основанных на формате JSON [5]).

Список литературы

1. Хоффман Л. Современные методы защиты информации. М.: Сов. радио, 1980.

2. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987.

3. Материал из Национальной библиотеки им. Н. Э. Баумана [Электронный ресурс]. URL: https://ru.bmstu.wiki/ACL_(Access_Control_List) (дата доступа 23.09.2020).

4. Ньюмен С. Создание микросервисов. СПб.: Питер, 2016.

5. Предлагаемый стандарт RFC 7519 [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc7519 (дата доступа 10.10.2020).

References

1. Hoffman L. *Sovremennyye metody zashchity informatsii* [Modern methods of information security]. Moscow, Sov. radio Publ., 1980.

2. Ayerland K., Rosen M. *Klasicheskoye vvedeniye v sovremennuyu teoriyu chisel* [A Classical Introduction to Modern Number Theory]. Moscow, Mir Publ., 1987.

3. *Material iz Natsional'noy biblioteki im. N. E. Baumana* [Material from the National Library N. E. Bauman] [Electronic resource]. Available at: https://ru.bmstu.wiki/ACL_(accessed 23.09.2020).

4. Newman S. *Sozdaniye mikroservisov* [Building Microservices]. St. Petersburg, Piter Publ., 2016.

5. *Predlagayemyy standart RFC 7519* [Proposed Standart RFC 7519] [Electronic resource]. Available at: https://tools.ietf.org/html/rfc7519 (accessed 10.10.2020).

Информация об авторах

Курилец Анастасия Витальевна – ассистент кафедры программной инженерии. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: oav@belstu.by

Смелов Владимир Владиславович – кандидат технических наук, доцент, заведующий кафедрой информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: smw@belstu.by

Горанин Николай – доктор наук, доцент кафедры «Информационные системы». Вильнюсский технический университет имени Гедиминаса (10223, Вильнюс, ул. Саулетекио, 11, Литовская Республика). E-mail: nikolaj.goranin@vgtu.lt

Information about the authors

Kurylets Anastasiya Vitalievna – assistant lecturer, the Department of Software Engineering. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: oav@belstu.by

Smelov Vladimir Vladislavovich – PhD (Engineering), Associate Professor, Head of the Ddepartment of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: smw@belstu.by

Goranin Nikolaj – DSc, Associate Professor, the Department of Information Systems. Vilnius Gediminas Technical University (11, Sauletekio str., 10223, Vilnius, Republic of Lituania). E-mail: nikolaj.goranin@vgtu.lt

Поступила после доработки 15.01.2021