ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ

УДК 004.94, 004.021, 004.27

ВЫБОР МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ СИСТЕМ АВТОМАТИЗАЦИИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

С.Е. Голиков[1], зав. лаб., Н.В. Серова-Нашева[2], к.т.н.

[1]Севастопольский институт банковского дела УБД НБУ
[2]Севастопольский национальный университет ядерной энергии и промышленности

Рассмотрены основные принципы информационной безопасности банковской ИТ инфраструктуры, состав систем управления доступом. Описаны преимущества и недостатки основных моделей разграничения доступа, которые могут быть использованы в банковских информационных системах. Показано, что использование гибридной модели доступа RBAC-ABAC позволяет создать оптимальную инфраструктуру управления доступом и удовлетворить динамически изменяющиеся потребности банковских организаций в области контроля доступа информационных систем.

Введение

Одной из приоритетных задач информационной безопасности банка является управление доступом к электронным ресурсам. Сердцевиной банковского финансового документооборота является автоматизированная банковская система, являющаяся большим и сложным многопользовательским приложением. Цели банковской организации достигаются скоординированными действиями всех ее сотрудников. Действия заранее планируются и распределяются в виде задач (функций и обязанностей). Состав задач и их распределение между персоналом может меняться вследствие [1]:

- изменения целей организации;
- оптимизации деятельности;
- адаптации деятельности под новые условия внутренней и внешней среды.

Распределение функций между сотрудниками предполагает предоставление каждому из них соответствующих ресурсов. В большинстве случаев наблюдается ситуация, когда предоставленные сотруднику полномочия превышают объем, необходимый для выполнения его обязанностей. Согласно отчету ORX Global Database за 2012 год [2], 75 % потерь в банковской сфере обусловлено влиянием человеческого фактора.

ИТ инфраструктура банка должна быть доступна не только для внутренних сотрудников, но и для клиентов, а в некоторых случаях и для поставщиков. Поскольку количество и разнообразие людей, которые должны иметь доступ, растет, становится очевидным, что традиционные процессы и системы управления безопасностью становятся уязвимыми. Нарушения системы безопасности приводит к возникновению «дыр», вследствие чего кредитное учреждение не может:

- своевременно предоставить пользователям системы требуемый доступ к ресурсам информационной системы;
- создавать учетные записи пользователей с необходимыми полномочиями;
- вовремя блокировать доступ к освобождаемым ресурсам.

Неэффективное управление пользовательскими привилегиями привело к принятию, например в США, целого ряда законов (Сайрбенса-Оксли, Грамма-Лича-Билли, HIPPA, FDA 21-CFR-11), направленных на усиление внутреннего аудита за системой безопасности предприятий.

До 1992 года существовали две основные модели управления доступом: модель принудительного управления доступом (MAC, mandatory access control) и модель дискретного управления доступом (DAC, discretionary access control). Данные модели были приняты в качестве стандарта Министерством обороны США. Модель MAC нашла применение в основном для контроля доступа в многоуровневых военных информационных системах, а DAC – во многих коммерческих операционных системах, включая Windows. В 1992 году Д. Феррайло и Р. Кун описали концепцию ролевого управления доступом (RBAC). Большой вклад в развитие классических моделей RBAC внесли Р. Садху, Е. Койен, С. Юман. В настоящее время существует стандартизованная Национальным институтом стандартов и технологий США модель RBAC. Для учета различных особенностей современных информационных систем предложено множество модификаций RBAC [3 - 5]. В странах СНГ развитием модели RBAC занимаются Д. Коллегов, Н. Семенова.

Таким образом, один из основных способов уменьшения операционного риска состоит в правильном распределении полномочий. Данный механизм в системах автоматизации банка представлен в виде системы управления и контроля доступа, реализующей модель доступа.

Постановка цели и задач научного исследования

Целью данной научной работы является выбор оптимальной для банковской автоматизированной системы модели управления доступом, обладающей свойствами абстрактности, простоты и адекватности моделируемой системе.

Для достижения поставленной цели необходимо рассмотреть основные модели управления доступом в отдельности и отметить преимущества и недостатки их самостоятельного и комплексного использования.

Решение поставленной задачи

Решение поставленной задачи необходимо начинать с рассмотрения основных моделей безопасности и их особенностей.

Современная банковская автоматизированная система представляет собой сложный программно-технический комплекс. Банки имеют сложную иерархическую организационную структуру, внутренние пользователи постоянно сталкиваются с проблемами доступа к определенным ресурсам в связи с динамической природой современных банков.

Модель управления доступом играет основную роль в системе безопасности информационной системы. Цель модели – выражение сути требований по безопасности к данной системе [6]. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации. Модель не накладывает ограничений на реализацию тех или иных механизмов защиты. Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе. Базовыми принципами обеспечения безопасности являются [7 - 9] (рис. 1):

- *доступность* – свойство ресурса системы, которое заключается в том, что пользователь и/или процесс, обладающий соответствующими полномочиями, может использовать ресурс в соответствии с правилами, установленными политикой безопасности, не дожидаясь дольше заданного (малого) промежутка времени, то есть когда он находится в виде, необходимом пользователю, в месте, необходимом пользователю, и в то время, когда он ему необходим;

- *целостность* – свойство информации, которое заключается в том, что информация не может быть модифицирована неавторизованным пользователем и/или процессом;

- *конфиденциальность* – свойство информации, которое заключается в том, что информация не может быть получена неавторизованным пользователем и/или процессом.

Рис. 1. Триада AIC

Инфраструктура управления доступом в информационных банковских системах должна состоять, как минимум, из четырех компонентов:

– идентификация пользователя (обычно в качестве идентификатора используется идентификатор логина пользователя);

– аутентификация пользователя, реализуемая при помощи паролей, маркеров безопасности, биометрической идентификации, запроса/ответа данных или комбинации факторов аутентификации;

– авторизация пользователей с помощью списков контроля доступа, членства в группах, ролей приложений и т.д.;

– аудит, регистрация доступа пользователей к системам данным.

Существует три основных модели безопасности – модель принудительного управления доступом (MAC), модель с управлением доступом по усмотрению пользователя (DAC), а также управление доступом на основе ролей. Недостатком модели DAC является то, что каждый объект должен иметь владельца, который может делать с ним все, что угодно, а также возможность передать право на чтение другим субъектам, не уведомляя об этом владельца. В банковских информационных системах владельцем всех ресурсов должна быть сама система. Кроме того, возникновение уязвимости, связанной с атаками «троянским конем», служит еще одной причиной отказа от применения данной модели. Управление доступом носит децентрализованный характер, пользователи – владельцы объекта сами управляют доступом к объектам и ресурсам. В модели MAC основной упор делается на конфиденциальность, но не решена проблема из-

менения классификации: уровень секретности остается неизменным. Однако применение данной модели в банковских информационных системах ограничено тем, что мандатная модель безопасности основывается на уровнях безопасности, которые априори должны существовать в предметной области. Однако банковская информационная модель не имеет изначально подобных ограничений, кроме того, в данной модели есть только два права доступа – чтение и запись, которых явно недостаточно для моделирования сложных финансовых процессов. Модель RBAC контролирует доступ пользователей на основе выполняемых ими задач (ролей). Роль есть семантическая конструкция, лежащая в основе политики ограничения доступом. Под ролью понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Роли позволяют получить конкретным лицам доступ к ресурсам в той степени, в какой это необходимо им для выполнения своих обязанностей. В модели RBAC используются следующие термины: пользователи, объекты, привилегии, роли, сессии, операции.

Под пользователями понимаются авторизованные пользователи системы, под объектами – ресурсы системы, доступ к которым регулируется с помощью RBAC. Привилегия – минимально возможное атомарное действие пользователя, которое подпадает под действие механизма разграничения доступа. Правила динамически расширяют логику статических ролей. Роль – это набор прав, определяющих, какими привилегиями и над какими объектами будет обладать пользователь, которому присваивается данная роль. Операция – составная часть роли, определяющая привилегию, подмножество объектов, обладающих данной привилегией, и разрешение или запрет на выполнение данного действия. Сессия – множество ролей данного пользователя в определенный промежуток времени. Одновременно может выполняться несколько сессий одного и того же пользователя. Процесс доступа пользователя к ресурсам в модели RBAC представлен на рис. 2.

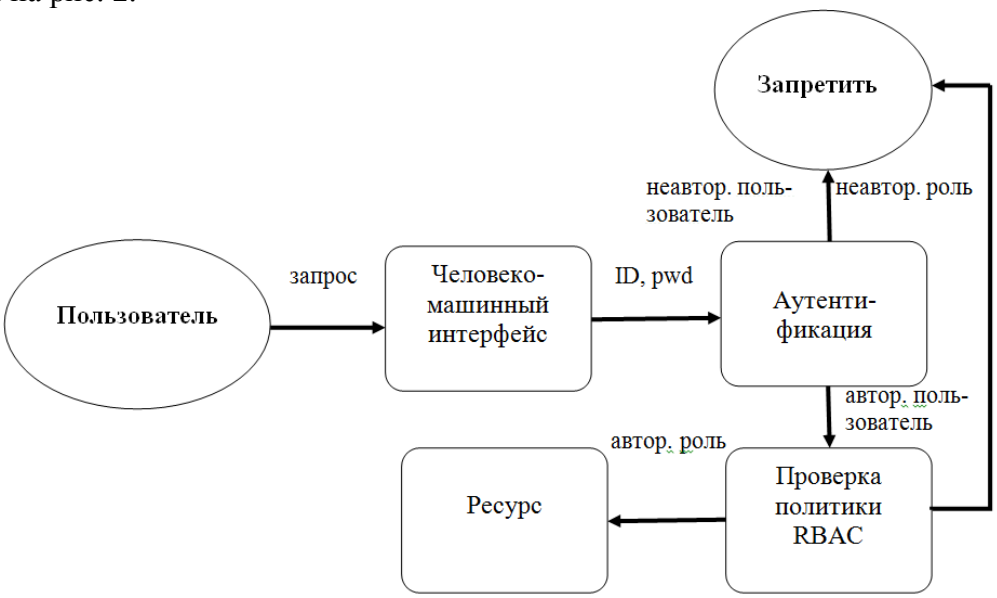

Рис. 2. Процесс доступа пользователя к ресурсам в модели RBAC

Процесс доступа состоит из следующих шагов:

1. Пользователь запрашивает доступ к ресурсу посредством человеко-машинного интерфейса (пользовательского интерфейса, файла данных, аппаратного устройства).

2. Служба аутентификации проверяет его учетные данные. В случае отсутствия прав пользователю отправляется сообщение и доступ не предоставляется.

3. Если пользователь прошел аутентификацию, дальше происходит проверка прав запрошенного доступа к объекту на основании присвоенной пользователю роли.

4. В случае успеха происходит предоставление права на доступ к ресурсу, в противном случае – отказ.

Основными элементами классической модели RBAC являются:

UA: авторизованные роли пользователей $\subseteq$ Пользователи $\times$ Роли .

PA: права доступа ролей $\subseteq$ Привилегии $\times$ Роли .

U-S: субъект-сессии пользователя $(\text{u} : \text{Пользователи}) \to 2^{\text{сессии}}$.

S-R: роль-сессии $(\text{s} : \text{сессии}) \to 2^{\text{роли}}$.

PRMS: привилегии $2^{(\text{объекты} \times \text{операции})}$.

$\text{Op} : (\text{p} \in \text{PRMS}) \to \{\text{op} \subseteq \text{Операции}\}$ – множество операций, связанных с привилегией p.

$\text{Ob} : (\text{p} \in \text{PRMS}) \to \{\text{op} \subseteq \text{OBS}\}$ – множество объектов, связанных с привилегией p.

CheckAccess – функция получения доступа. Возвращает TRUE, если доступ разрешен, в противном случае – FALSE.

$$\text{CheckAccess}(\text{s}, \text{op}, \text{ob}) = (\exists\, \text{r} \in \text{ROLES} : \text{r} \in \text{S} - \text{R}(\text{s}) \wedge ((\text{op}, \text{ob}), \text{r}) \in \text{PA}).$$

CheckAccess = TRUE, если может быть разрешен доступ к операции op над объектом ob пользователю с ролью r в сессии s.

Ролевая модель управление доступом по сравнению с предыдущими двумя моделями лучше подходит для банковских учреждений, в которых существует четкое разделение полномочий между работниками, а работники, занимающие одни и те же должности, обладают одними и теми же полномочиями. Механизм ролевого управления доступом может быть легко использован для применения правила разделения обязанностей, что требуется нормативными документами НБУ [10]. Разделение обязанностей в банках используется в целях предотвращения внутреннего мошенничества, например, для платежных документов запрещается совмещение одному лицу обязанностей операциониста и бухгалтера. Кроме того, в правилах присвоения ролей мы можем определить только одного администратора или ограничить доступ к определенным объектам для разных пользователей. Так, работники отделения 1 смогут работать только со счетами, которые закреплены за ними, но не смогут выполнять операции со счетами, закрепленными за отделением 2. Для этого мы можем совместить модель RBAC и модель ABAC (атрибутивная модель управления доступом), введя правила, которые, используя различные аттрибуты объектов, смогут выполнять функцию разделения ответственности. Тогда набор привилегий, присвоенных пользователю, будет определяться по формуле

$$\text{Привилегии} = \text{UserRole} \cdot \text{Operation} + \text{UserRules},$$

где UserRole – пользовательские роли;

Operation – операции;

UserRules – пользовательские права.

Теперь для развертывания ролевой модели достаточно закрепить за пользователем одну или несколько ролей и определить правила, чтобы определить все привилегии, которыми он должен обладать.

Для недопущения конфликтов ролей необходимо использовать правила одного знака: например, только разрешающих. Тогда во множестве ролей, составленном только из разрешающих правил, присвоение пользователю еще одной роли приводит только к расширению его прав доступа, не накладывая ограничений на существующие.

Банковские учреждения имеют иерархическую структуру, поэтому целесообразно применять модель ролевого управления доступом с иерархией сущностей. Тогда сотрудники вышестоящих подразделений смогут получать права доступа к данным нижестоящих подразделений. В то же время сотрудники нижестоящих подразделений не смогут без специального разрешения получить доступ к данным вышестоящих подразделений. При использовании иерархического ролевого управления доступом набор привилегий, присвоенных пользователю, будет определяться формулой

$$\text{Привилегии} = \text{Level}(\text{UserRole} \cdot \text{Operation}) + \text{UserRules}.$$

В банках множество выполняемых функций ограничено временными рамками, например, прием-передача платежей через СЭП, работа в системе SWIFT, ДБО в некоторых банках и т.п. В таких случаях роль должна быть доступна только в течение определенного временного интервала. Расширение модели RBAC, поддерживающее данные требования, получило название TRBAC. Еще одним полезным расширением модели RBAC в контексте банковских информационных систем является модель SRBAC, позволяющая ограничивать/разрешать доступ в зависимости от места нахождения члена роли. Совместное использование TRBAC и SRBAC позволяет строить правила, разрешающие, например, доступ к определенным ресурсам с 09:00 до 17:00 с понедельника по пятницу только из офиса. С учетом времени и месторасположения набор привилегий пользователя определяется формулой

$$\text{Привилегии} = \text{Location}(\text{Time}(\text{Level}(\text{UserRole} \cdot \text{Operation}))) + \text{UserRules}.$$

Такой подход более гибкий, чем чистая модель RBAC, так как позволяет строить модели доступа на основе атрибутов субъекта (ABAC). Отпадает необходимость в создании отдельных ролей, можно просто изменять атрибуты правил. Платой за гибкость является усложнение модели. В случае n атрибутов мы имеем дело с 2^n возможными комбинациями значений. Используя чистую модель RBAC легко администрировать права, но требуется много времени для разработки самой модели разграничения доступа. И, наоборот, модель ABAC проста в настройке, однако, анализ и изменение прав пользователей может оказаться проблематичным. Для банковских информационных систем компромиссом является объединение моделей RBAC и ABAC для того, чтобы воспользоваться их сильными сторонами.

В таблице приведены возможные комбинации моделей RBAC и ABAC.

В моделях ABAC-основной и гибридной ABAC-RBAC идентификатор пользователя не участвует в принятии решения о предоставлении доступа, поэтому данные модели можно использовать в случаях определения прав доступа для анонимных пользователей.

Проанализировав вышеприведенную таблицу, в быстро меняющейся среде, какой является банковская система, интерес представляют только три комбинации:

– RBAC-A, динамические роли. Традиционная структура роли сохраняется, но предоставляется возможность динамически изменять атрибуты роли. Например, ввести ограничение по времени на использование роли или на число одновременно работающих администраторов системы, хотя административные роли могут иметь несколько пользователей. Динамическое изменение можно реализовать как отдельный слой поверх обычной модели RBAC;

– RBAC-A на основе атрибутов. В данной модели имя роли является одним из атрибутов. В отличие от обычной модели RBAC, роль не является набором ограничений, а только названием атрибута. Недостатком данной модели является сложность администрирования;

– RBAC-A на основе ролей. В данной модели к ограничениям RBAC добавляются атрибуты субъекта. Правила, использующие атрибуты, сужают действия ролей. Однако появляется возможность очень точно настроить пользовательские разрешения.

Таблица

Комбинации моделей RBAC и ABAC

U	R	A	Модель	Отображение прав доступа
0	0	0	Не определена	-------
0	0	1	ABAC-основная	$A_1,A_2,\ldots A_n \rightarrow$ permissions
0	1	0	Не определена	-------
0	1	1	Гибридная ABAC-RBAC	R, $A_1,A_2,\ldots A_n \rightarrow$ permissions
1	0	0	Списки доступа	U $\rightarrow$ permissions
1	0	1	ABAC-ID	U, $A_1,A_2,\ldots A_n \rightarrow$ permissions
1	1	0	RBAC-основная	U $\rightarrow$ R $\rightarrow$ permissions
1	1	1	RBAC-A, динамические роли	U, $A_1,A_2,\ldots A_n \rightarrow$ R $\rightarrow$ permissions
1	1	1	RBAC-A на основе атрибутов	U, R, $A_1,A_2,\ldots A_n \rightarrow$ permissions
1	1	1	RBAC-A на основе ролей	U $\rightarrow$ R $\rightarrow A_1,A_2,\ldots A_n \rightarrow$ permissions

Примечание. U – пользователь/ID субъекта; R – роль; A – атрибуты.

В работе [10] сформулированы основные свойства атрибутивных моделей управления доступом:

1. В модели имеются множества сущностей E, субъектов $S \subset E$, прав доступа R и объектов – параметров $P = \{p_1,\ldots,p_m\} \subset E$. Каждой сущности поставлено в соответствие некоторое множество атрибутов – переменных с конечными множествами значений, и набор значений атрибутов сущности e обозначен как $A(e)$. Каждой тройке $(s,e,r) \in S \times E \times R$ поставлены в соответствие некоторые параметры $q_1,\ldots,q_n \in P$ и предикат, зависящий от $A(s), A(e), r, A(p_1),\ldots,A(p_k)$ так, что субъект $s \in S$ получает право доступа $r \in R$ к сущности $e \in E$, когда истинен этот предикат.

2. В момент времени t состояние модели определяется как

$$G_t = (E_t, V_t, (p_1, A(p_1)),\ldots,(p_m, A(p_{m1}))),$$

где E_t – множество сущностей системы в момент времени t и V_t – множество всех реализаций прав доступа субъектов к сущностям, которые имеют место в момент времени t.

Множество V_t состоит из элементов v_t, где $v_t = ((s, A(s)), (e, A(e)), r)$, $s \in S$, $e \in E$, $r \in R$. Таким образом, состояние банковской информационной системы в модели определяют сущности, текущая реализация прав доступа субъектов к сущностям вместе с их значениями атрибутов и значения атрибутов объектов – параметров. Траекторией функционирования модели называется конечная последовательность состояний $G_0,\ldots,G_t$, где G_0 – начальное состояние, G_i получается из G_{i-1} либо при появлении новой сущности системы, либо при изменении значения атрибута некоторого объекта – параметра, либо при получении субъектом некоторого права доступа к сущности. Множество всех траекторий функционирования информационной системы с начальным состоянием G_0 обозначается $P(G_0)$.

3. В соответствии с политикой безопасности $P(G_0)$ разбивается на два непересекающихся подмножества: $LP(G_0)$ − разрешенных и $NP(G_0)$ – неразрешенных траекторий, и определяются множества L_a, N_a, L_r, N_r, L_f, N_f, разрешенных и запрещенных доступов, прав доступов и информационных потоков соответственно. Нарушение безопасности информационной системы определяется как переход в состояние, в котором имеется запрещенный доступ из N_a или на траектории к которому произошло получение запрещенного права доступа из N_r, или реализован запрещенный информационный поток из множества N_f.

Таким образом, исходя из вышесказанного, для банковских информационных систем целесообразно использовать комбинированную модель RBAC-ABAC. Подобный подход позволяет существенно упростить разработку структуры ролей. Например, если у нас имеется 7 статических (например, балансовый счет, тип счета, вид счета, признак счета, вид начисляемого процента, код банковского продукта, код клиента) и 3 динамических атрибута (например, время доступа, местоположение, категория пользователя), то в базовой модели RBAC нам потребуется описать 1024 роли, а в комбинированной – максимум 128 ролей и 4 правила.

Выводы

Проведенный анализ основных моделей, применяемых для разграничения доступа, позволил выделать базовые принципы обеспечения безопасности банковских информационных систем, их преимущества и недостатки. Предложено использование гибридной модели разграничения доступа, которая позволяет сохранить преимущества как ролевой, так и атрибутивной моделей и избавиться от присущих им недостатков, тем самым уменьшая вероятность возникновения операционных рисков.

Дальнейшие перспективы связаны с созданием прототипа системы разграничения доступа системы автоматизации банка.

ВИБІР МОДЕЛІ УПРАВЛІННЯ ДОСТУПОМ СИСТЕМ АВТОМАТИЗАЦІЇ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

С.Є. Голиков, Н.В. Серова-Нашева

Розглянуто основні принципи інформаційної безпеки банківської IT-інфраструктури, склад систем управління доступом. Описані переваги і недоліки основних моделей розмежування доступу, які можуть бути використані в банківських інформаційних системах. Показано, що використання гібридної моделі доступу RBAC-ABAC дозволяє створити оптимальну інфраструктуру управління доступом і задовольнити динамічно змінюющиеся потреби банківських організацій в галузі контролю доступом інформаційних систем.

CHOOSING an ACCESS CONTROL MODEL of the BANKING INFORMATION SYSTEM

S. Golikov, N. Serova-Nasheva

Considered the basic principles of information security of the banking IT infrastructure, the composition of access control systems. Describes the benefits and disadvantages of the basic access control models, which can be used in the banking information system. It is shown that the use of a hybrid aceess model RBAC-ABAC allows to adjust the access control infrastructure and to meet the changing needs of the banking institutions in the field of access control information systems.

Список использованных источников

1. Оранжевая книга [Электронный ресурс]. – Режим доступа: http://orange-webstudio.com/bezopasnost/upravlenie-siste.html
2. ORX Report on Operational Risk Loss Data [Электронный ресурс]. – Режим доступа: http:// www.orx.org2012
3. *Kuhn D.R.* Adding attributes to role-based access control / D.R. Kuhn, E.J. Coyne. T.R. Weil // IEEE Computer. − 2010. − No. 43 (6). − P. 79 – 81.
4. *Joshi J.* A Generalized Temporal Role-Based Access Control Model / J. Joshi, E.A. Bertino, U. Latif, A. Ghafoor // IEEE Trans. Knowledge and Data Engineering. - 2005. − N. 17 (1). − P. 4 – 23.
5. *Bertion E.* GEO-RBAC: A Spatially Aware RBAC / E. Bertion, B. Catania, M.L. Damiani // Proc. 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweeden, June 2005. − P. 29 – 37.
6. *Амелин Р.В.* Информационная безопасность [Электронный ресурс]. – Режим доступа: http://nto.immpu.sgu.ru/sites/default/files/3/__77037.pdf
7. *Соколов А.В.* Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. − 187 с.
8. The AIC TRIAD [Электронный ресурс]. – Режим доступа: http://www.infosecschool.com/aic-triad_cia-triad/
9. СОУ Н НБУ 65.1 СУІБ 2.0:2010. Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою (ISO/IES 27002:2005, MOD) [Електронний ресурс]. – Режим доступа: http://www.zakon.rada.gov.ua
10. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

Надійшла до редакції 28.11.2013 р.

УДК 539.1.074: 004.315

ВЕРОЯТНОСТНЫЙ ПАРАЛЛЕЛЬНЫЙ СУММАТОР

Н.Е. Сапожников, д.т.н., проф., Д.В. Моисеев, к.т.н.

Севастопольский национальный университет ядерной энергии и промышленности

Рассматривается решение задачи выполнения арифметической операции сложения параллельных данных, представленных в виде вероятностных отображений. Приводятся математический аппарат и функциональные схемы параллельного вероятностного сумматора, выполняющего арифметическую операцию сложения параллельных данных, представленных в вероятностной форме.

Введение

В настоящее время вопросам вероятностного представления и преобразования данных посвящен ряд работ [1 - 4]. Анализ данных работ позволил сделать вывод о том, что вероятностная форма представления информации, применяемая до настоящего времени лишь в достаточно узкой специализированной области, может быть использована в различных областях экономики, где необходимо осуществлять обработку большого объема данных [5].