УДК 004.056.53

В. М. Черненький, Гхаиад Иссам

МЕТОДИКА АДМИНИСТРИРОВАНИЯ ЗАЩИТЫ ДОСТУПА К ДАННЫМ В АСУП

Рассмотрена проблемам обеспечения защиты доступа к данным в любых информационных системах. Особенностью предлагаемого подхода является создание распределенного комплекса методов по защите каждого данного, включая создание дополнительных ключевых записей, также обеспеченных защитой. Предложен теоретический аппарат, описывающий этапы создания и эксплуатации системы защиты в целом. Рассмотрены операции преобразования цепочек и показатели эффективности распределения методов защиты.

Проблема защиты информации от несанкционированного доступа возникает, как только предприятие начинает активно внедрять и использовать информационные технологии в процессе своей деятельности. К настоящему времени разработаны и предлагаются к применению методы защиты информации, основанные на различных подходах.

Часть таких методов достаточно дорога в эксплуатации, поскольку требует высокопрофессионального обслуживающего персонала, другие имеют невысокую надежность, третьи не поддаются администрированию. В то же время бóльшая часть предприятий мелкого и среднего уровня нуждается в эффективном, недорогом и управляемом методе, обеспечивающем защиту доступа к данным в ходе эксплуатации автоматизированной системы управления предприятием (АСУП).

Рассмотрим теоретические основы подхода к решению указанной проблемы, основанного на создании методики администрирования защиты доступа к данным, как на этапе проектирования информационной системы, так и на этапе ее эксплуатации.

Исходные положения. В основе функционирования предприятия в АСУП лежат описания бизнес-процессов различных аспектов его деятельности. Схематично бизнес-процесс можно представить двудольным графом, содержащим вершины “Данные” и “Процедуры” (рис. 1).

Пользователи (один или несколько) для выполнения бизнес-процесса должны получить доступ к данным как на считывание, так и на запись необходимой информации. Так, для выполнения процедуры Пр_1 необходимо получить данные D_1 и D_2. Именно этот аспект в дальнейшем изложении берется за основу разрабатываемой методики администрирования.

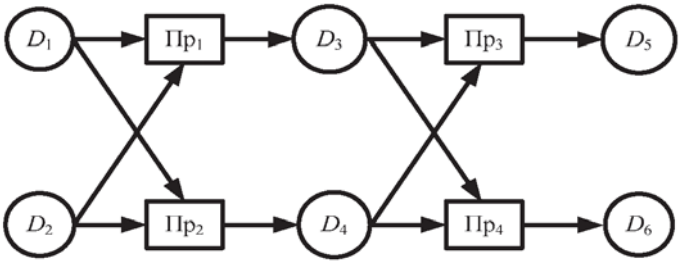

Рис. 1. Пример представления бизнес-процесса

Введем понятие расщепленного данного. Данное считается расщепленным, если представлено в виде связанной последовательности двух подданных: исходного и конечного. Например, данные о зарплате сотрудника предприятия можно представить в виде подданных: исходного — "Фамилия" и конечного — "Сумма зарплаты". Отношения между этими подданными могут быть произвольными. Другой пример — число деталей различной номенклатуры на складе. Исходное подданное — номенклатура детали, конечное подданное — число деталей. Исходное и конечное подданные связаны некоторым отношением. Таким образом, данное можно представить в виде линейного графа, содержащего две вершины (рис. 2). Такой граф будем называть *исходным элементом*.

Назовем вершину A исходной, а вершину B конечной. Стрелка от A к B означает наличие отношения, представленного в виде указателей и позволяющего для каждого элемента из A найти соответствующий элемент в B.

Формализация. Предположим, что подданные A и B защищены от несанкционированного доступа некоторыми методами. Это означает, что, прежде чем мы получим доступ к конкретному подданному, мы должны преодолеть некоторую защитную оболочку. Назовем эту оболочку капсулой. Рассмотрим вершину Q исходного элемента, капсула $K(Q)$ которой характеризуется следующими параметрами:

$$K(Q) = \langle M(Q),\ R(Q),\ S(Q),\ P(Q) \rangle,$$

где $M(Q)$ — метод защиты; $R(Q)$ — способ его реализации; $S(Q)$ — стоимость реализации метода; $P(Q)$ — вероятность несанкционированного преодоления защиты, обеспеченной методом $M(Q)$.

Рис. 2. Исходный элемент

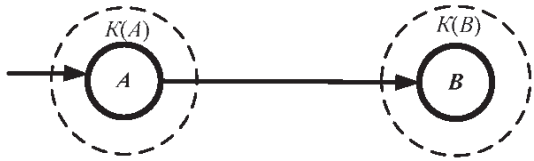

Рис. 3. Капсулированный исходный элемент

В дальнейшем вероятность несанкционированного преодоления защиты $P(Q)$ будем называть мерой опасности.

С учетом защиты, граф связанности двух подданных будет иметь вид, показанный на рис. 3. Вершины *A* и *B* представляют собой подданные, капсулы обозначены штриховыми кружками вокруг подданных. Таким образом, чтобы получить необходимую информацию, следует преодолеть капсулу $K(A)$, найти искомый элемент и соответствующий указатель на *B* и преодолеть капсулу $K(B)$. Стрелка на подданное *A*, не исходящая из вершины, означает, что нам не нужны указатели, достаточно лишь получить доступ к *A* через капсулу $K(A)$. При обычной работе с данными такой вход имеют лишь исходные вершины.

В предположении, что $M(A)$ и $M(B)$, соответствующие капсулам $K(A)$ и $K(B)$, независимы и не связаны между собой, можно вычислить меру опасности цепочки (см. рис. 3) как

$$P(A, B) = P(A) \times P(B).$$

Действительно, доступ к информации в *A* и получение указателей на *B* не позволяют найти необходимые данные в *B* без преодоления капсулы $K(B)$. В то же время преодоление капсулы $K(B)$ и получение информации в *B* без преодоления капсулы $K(A)$ предоставляет нам лишь обезличенные данные, не позволяющие определить их владельцев. Только преодоление капсул $K(A)$ и $K(B)$ одновременно дает возможность решить поставленную задачу. Поскольку $P(A)$ и $P(B)$ меньше единицы, то $P(A, B)$ меньше каждой из них. Таким образом, расщепление данных и последующее капсулирование позволяют *снизить* меру опасности несанкционированного получения защищаемых данных.

Полученный вывод позволяет предложить расширенную схему защиты данного путем введения дополнительных вершин в цепочку от *A* к *B*, содержащих только указатели на информацию в соседней вершине. Назовем такие вершины ключевыми.

На рис. 4 приведен пример цепочки, содержащей исходную вершину *A*, искомую вершину B и две ключевые вершины *C* и *D*.

Аналогично приведенному рассуждению, учитывая независимость методов защиты в каждой капсуле, можно вычислить меру опасности

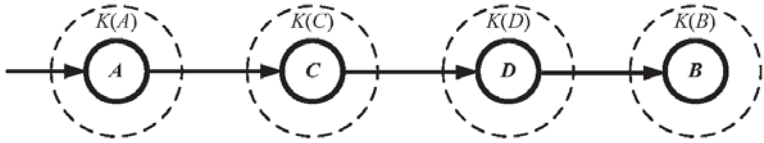

Рис. 4. Цепочка исходного элемента с ключевыми вершинами

получения информации в A и B по цепочке A, C, D, B как

$$P(A, C, D, B) = P(A) \times P(C) \times P(D) \times P(B).$$

Очевидно, что мера опасности в рассматриваемой цепочке будет меньше, чем в предыдущем случае.

Таким образом, предложенный подход позволяет защитить не только сами данные, но и значительно усложнить в случае несанкционированного доступа процедуру связности элементов данных между собой, поскольку получение доступа не ко всем вершинам цепочки не позволяет соотнести одни элементы информации с другими.

Анализ связности методов. До сих пор предполагалось, что методы защиты в каждой капсуле разные и не связаны между собой. Однако практика показывает, что нередко методы защиты близки друг другу или же отличаются только параметрическими настройками. Вернемся к рассмотрению цепочки, приведенной на рис. 4. Предположим, что методы $M(A)$ и $M(B)$ коррелированны, т.е. каким-либо образом связаны между собой, например, построены по общему алгоритму и различаются лишь параметрами, и используют схожие схемы защиты. Для оценки коррелированности методов $M(A)$ и $M(B)$ введем понятие показателя связности $W(A, B)$, принимающего значения на $[0, 1]$. Предположим, что большее значение показателя связности соответствует большей степени коррелированности. Так, значение $W = 0$ соответствует полному отсутствию связности методов, в то время как значение $W = 1$ — полному сходству методов.

С учетом сказанного, введем понятие действительной меры опасности $P(Q)_{\text{дейст}}$ преодоления капсулы $K(Q)$ после преодоления капсулы $K(Q_1)$:

$$P(Q)_{\text{дейст}} = P(Q)^{1-W(Q_1,Q1)}.$$

Такое определение меры опасности для двух связанных вершин позволяет получить теоретически корректные значения в двух крайних точках: $W = 0$ и $W = 1$ (рис. 5). Так, при $W = 0$ мера опасности вершины Q определяется своим методом защиты и равна $P(Q)$. При $W = 1$ и жесткой коррелированности метода защиты $M(Q)$ в случае "взлома" метода защиты вершины Q_1 мера опасности вершины Q равна 1, что означает ее полную незащищенность.

Для цепочки, приведенной на рис. 3, меру опасности для получения информации в B через информацию в A можно определить, как

$$P(A,\, B) = P(A) \times P(B)_{\text{дейст}},$$

где $P(B)_{\text{дейст}} = P(B)^{1-W(A,\,B)}$.

В случае, когда $W(A,\, B) = 0$ получим

$$P\,(A,\, B) = P\,(A) \times P\,(B)\,,$$

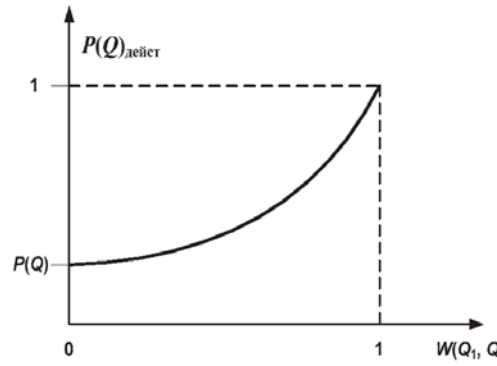

Рис. 5. Действительная мера опасности

что соответствует формуле при независимых методах защиты.

В случае, когда $W\,(A,\, B) = 1$, т.е. методы защиты одинаковы, имеем

$$P\,(A,\, B) = P\,(A)\,.$$

Полученный результат соответствует практике и объясняет следующее: если злоумышленник преодолел защиту капсулы $K\,(A)$, то защита капсулы $K\,(B)$ им преодолевается автоматически и не служит препятствием для доступа к данными в B.

Все значения W, которые больше нуля, повышают действительную меру опасности.

Рассмотрим цепочку из трех вершин (рис. 6).

Здесь показаны подданные A и C, ключевая вершина B, капсулы $K\,(A)$, $K\,(B)$, $K\,(C)$, а также показатели связности методов защиты в капсулах $W\,(A,B)$, $W\,(B,C)$, $W\,(A,C)$. Если преодолены капсулы $K\,(A)$ и $K\,(B)$, то можно преодолеть и капсулу $K\,(C)$, используя опыт преодоления метода $M\,(A)$ капсулы $K\,(A)$ или опыт преодоления метода $M\,(B)$ капсулы $K\,(B)$.

Таким образом, необходимо ввести понятие эквивалентного показателя связности $W\,(C)_{\text{экв}}$, учитывающего связность метода $M\,(C)$ и возможно преодоленных методов $M\,(A)$ и $M\,(B)$.

Для вывода формулы интерпретируем показатель связности $W\,(Q_1, , Q$ как вероятность преодоления защиты вершины Q при условии, что защита вершины Q_1 преодолена.

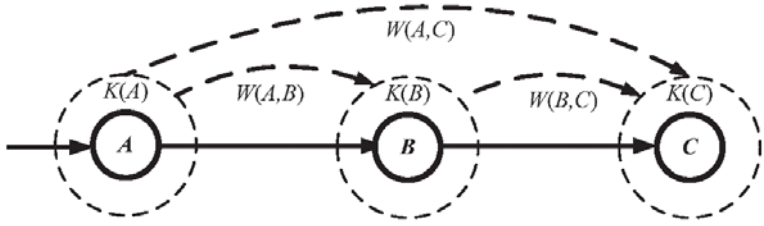

Рис. 6. Цепочка с ключевой вершиной

Поскольку W — показатель связности, значение которого лежит в интервале $[0,1]$, то выражение $(1-W)$ можно рассматривать, как показатель несвязности. Произведение показателей несвязности $(1-W(A,C))\times(1-W(B,C))$ можно интерпретировать как показатель одновременной несвязности.

Тогда показатель $W_{\text{экв}}$, являющийся дополнением одновременной несвязности до 1, можно интерпретировать, как показатель любого варианта связности.

Таким образом, получаем значение $W(C)_{\text{экв}}$ в виде следующей свертки:

$$W(C)_{\text{экв}} = 1-(1-W(A,C))\times(1-W(B,C)).$$

Исследуем свойства предлагаемой свертки.

1. Пусть любой из показателей связности ($W(B,C)$ или $W(A,C)$) равен единице.

Тогда $W_{\text{экв}}=1$. Этот результат соответствует представлению о том, что если метод $M(C)$ является одним из уже преодоленных методов $M(A)$ или $M(B)$, то эквивалентная связность тоже равна единице.

2. Пусть один из показателей связности, например $W(A,C)$, равен нулю.

Тогда $W_{\text{экв}}=W(B,C)$. Этот результат соответствует представлению о том, что если метод $M(C)$ не зависим от $M(A)$, то его зависимости определяются лишь зависимостью от $M(B)$.

3. Пусть оба показателя связности равны нулю.

Тогда $W_{\text{экв}}=0$. Этот результат соответствует представлению о том, что если метод $M(C)$ не зависит от $M(A)$ и $M(B)$, то его нужно рассматривать как совершенно независимый.

Таким образом, действительная мера опасности вершины C имеет вид

$$P(C)_{\text{дейст}} = P(C)^{1-W(C)_{\text{экв}}},$$

далее получим

$$P(C)_{\text{дейст}} = P(C)^{(1-W(A,C))\times(1-W(B,C))}.$$

В терминах введенных понятий меру опасности цепочки A,B можно представить как

$$P(A,B) = P(A)\times P(B)_{\text{дейст}},$$

где $P(B)_{\text{дейст}} = P(B)^{1-W(A,B)}$.

Мера опасности цепочки A,B,C

$$P(A,B,C) = P(A,B)\times P(C)_{\text{дейст}},$$

тогда, получим

$$P(A,B,C) = P(A)\times P(B)_{\text{дейст}}\times P(C)_{\text{дейст}}.$$

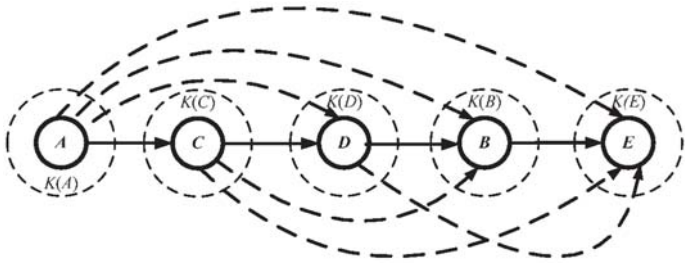

Рис. 7. Транзитивное замыкание по цепочке

Окончательно имеем

$$P(A,B,C) = P(A) \times P(B)^{1-W(A,B)} \times P(C)^{(1-W(A,C))\times(1-W(B,C))}.$$

Общий случай. Обобщая полученные результаты, можно утверждать, что в общем случае взаимосвязь методов защиты данных в капсулах можно рассматривать как направленное транзитивное замыкание по цепочке в целом. На рис. 7 приведен пример транзитивного замыкания по цепочке из пяти вершин.

Мера опасности по каждой вершине зависит от числа входящих в нее связей, что соответствует степени связности метода защиты вершины с методами защиты предыдущих вершин. Так, защита вершины B связана с методами защиты вершин A, C, D.

Рассмотрим общий случай взаимозависимости методов защиты для одной вершины цепочки. На рис. 8 изображена вершина Z, которая связана по методу защиты с вершинами $X_1, X_2, X_3, \ldots, X_n$, входящими в состав одной цепочки.

Тогда меру опасности вершины $K\,(Z)$ можно представить как

$$P(Z)_{\text{дейст}} = P(Z)^{1-W(Z)_{\text{экв}}},$$

где $W(Z)_{\text{экв}} = 1 - (1 - W(X_1, Z)) \times (1 - W(X_2, Z)) \times \ldots$ $\ldots \times (1 - W(X_n, Z))$ или

$$W\,(Z)_{\text{экв}} = 1 - \prod_{i=1}^{n} (1 - W\,(X_i, Z)).$$

Если вершины $X_1, X_2, X_3, \ldots, X_n, Z$ входят в состав одной цепочки и $X_1, X_2, X_3, \ldots, X_n$ предшествуют вершине Z, то величину $W\,(Z)_{\text{экв}}$ будем называть транзитивным эквивалентным показателем связности для вершины Z и обозначать как $W\,(Z)_{\text{экв.транз}}$.

Так, для вершины *B* (см. рис. 7), связанной с методами защиты вершин *A*, *C* и *D*, транзитивный эквивалентный показатель связности имеет вид

$$W(B)_{\text{экв.транз}} = 1 - (1 - W(A,B))\times \\ \times (1 - W(C,B)) \times (1 - W(D,B)).$$

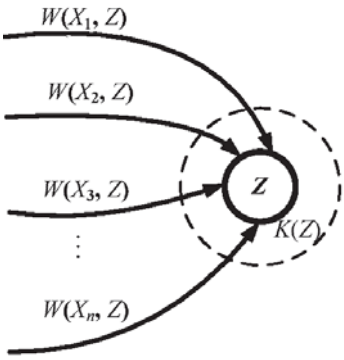

Рис. 8. Мера опасности для отдельной вершины в общем случае

Если же вершины $X_1, X_2, X_3, \ldots, X_n$ являются вершинами различных произвольных цепочек, то величину $W(Z)_{\text{экв}}$ будем называть ситуативным эквивалентным показателем связности для вершины Z и обозначать как $W(Z)_{\text{экв.ситуат}}$ (рис. 9).

Таким образом, при анализе *конкретной* цепочки будем пользоваться понятием транзитивного эквивалентного показателя связности, а при анализе защищенности конкретной вершины в условиях связности методов защиты всех вершин всех цепочек системы — понятием ситуативного эквивалентного показателя связности.

На рис. 10 приведена схема методики проектирования защиты заданной совокупности данных. Необходимая совокупность данных определяется описанием бизнес-процессов предприятия. Выделенные данные рассматриваются как мегаданные, и к ним прилагаются приведенные ранее методы анализа и преобразования.

В результате реализации методики получаем оптимальный вариант распределения методов защиты по цепочкам всех мегаданных. При этом используем понятие транзитивного эквивалентного показателя связности.

Администратор безопасности в ходе эксплуатации информационной системы имеет возможность контролировать степень защищенности каждого данного в ходе обнаружения угроз безопасности или противоправных действий. При этом алгоритм его действий соответствует приведенной методике с той лишь разницей, что при подсчете всех характеристик используется ситуативный эквивалентный показатель связности.

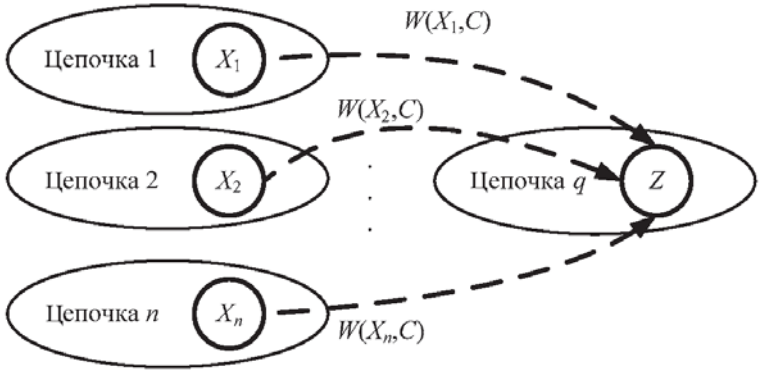

Рис. 9. Мера опасности для отдельной вершины из разных цепочек

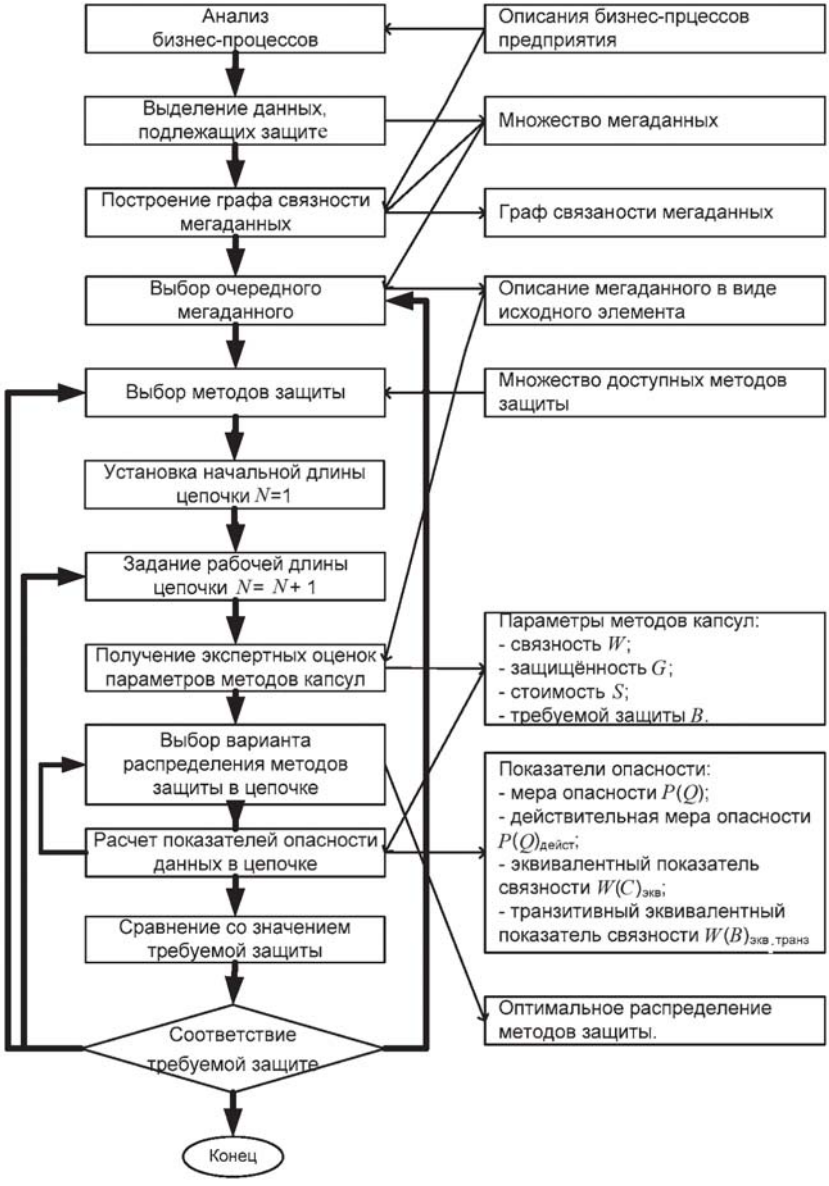

Рис. 10. Схема методики проектирования системы защиты данных

Выводы. 1. Показано, что при планировании состава и размещения данных целесообразно проводить их фрагментацию, вводить дополнительные ключевые вершины, защищая каждый фрагмент и вершину отдельной капсулой.

2. Предложен метод определения показателей защищенности данных с учетом взаимосвязанности и взаимозависимости методов защиты каждого элемента мегаданных.

3. Предложена методика проектирования системы защиты данных на предприятии.

СПИСОК ЛИТЕРАТУРЫ

1. Галатенко В. Информационная безопасность — основы // Системы управления базами данных. – 1996. – № 1.
2. Хмелев Л. Оценка эффективности мер безопасности, закладываемых при проектировании электронно-информационных систем // Тр. науч.-техн. конф. “Безопасность информационных технологий”. Пенза, июнь 2001.
3. Петренко С. А., Курбатов В. А. Политика информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.
4. Домарев В. В. Безопасность информационных технологии. Системный подход. – К.: ООО “ТИД “ДС”, 2004. – 992 с.
5. Садеринов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учеб. пособ. 2-е изд. – М.: Изд.-торг. корпорация “Дашков и К”, 2005. – 336 с.
6. Москвин Б. В. Теория принятия решений. – СПб.: Изд-во ВКА им. А.Ф. Можайского, 2005.
7. Черненький М. В. Проблемы информационной безопасности в банковских системах: Учеб. пособ. – М.: ООО “Эликс+”, 2003, – 132 с.

Статья поступила в редакцию 4.10.2007

Валерий Михайлович Черненький родился в 1941 г., окончил МВТУ им. Н.Э. Баумана в 1964 г. Д-р техн. наук, профессор, заведующий кафедрой “Системы обработки информации и управления” МГТУ им. Н.Э. Баумана. Академик Международной академии информатизации. Автор свыше 110 научных работ в области моделирования и системного анализа.

V.M. Chornenkiy (b. 1941) graduated from the Bauman Moscow Higher Technical School in 1964. D. Sc. (Eng.), professor, head of “Systems of Data Processing and Control” department of the Bauman Moscow State Technical University. Academician of the International Academy of Information Technologies. Author of more than 110 publications in the field of modeling and system analysis.

Гхаиад Иссам родился в 1967 г., окончил университет Алеппо (Сирия) в 1992 г. Аспирант кафедры “Системы обработки информации и управления” МГТУ им. Н.Э. Баумана. Специализируется в области систем защиты информации.

Ghaiad Issam (b. 1967) graduated from the University (Syria) in 1992. Post-graduate of “Systems of Information Processing and Control” department of the Bauman Moscow State Technical University. Specializes in the field of systems of information protection.