УДК 004.04

В.Е. Мухин

Оценка рисков защищенности распределенных компьютерных систем в процессе анализа ситуаций и принятия решений

Описаны основные компоненты безопасности распределенных компьютерных систем и понятия, используемые при оценке рисков защищенности. Предложен подход к формализации представления ядра управления заданиями таких систем с использованием *UML*-диаграмм. Приведены оценки рисков защищенности и восстановления ее уровня.

The main security components of the distributed computer systems (DCS), as well as the concepts used for security risks assessing are described. An approach to formalization of the DCS task control core using the UML-diagrams is suggested. The security risks assessments and the restoration of its level are given.

Описано основні компоненти безпеки розподілених комп'ютерних систем та поняття, що використовуються для оцінки ризиків захищеності. Запропоновано підхід до формалізації подання ядра управління завданнями таких систем з використанням *UML*-діаграм. Наведено оцінки ризиків захищеності та відновлення її рівня.

Введение. В распределенных компьютерных системах (РКС) существует значительное число уязвимостей, используемых агентами вторжений для организации атак с целью несанкционированного доступа (НСД) к информации. В свою очередь известен ряд методов и средств обнаружения вторжений и соответствующих *host*- и *network*-ориентированных систем мониторинга и предотвращения вторжений [1]. Стандарт *ISO*-15408 [2] определяет требования к специальным мерам по анализу рисков защищенности на различных этапах проектирования, разработки, внедрения и сопровождения средств защиты информации от НСД, а также функции владельцев информации и владельцев РКС по защите от возможных угроз и вторжений. Вопросы анализа рисков защищенности РКС – актуальное направление в области построения эффективных средств защиты информации.

Основные компоненты безопасности РКС

Безопасность РКС основывается на защите ее ресурсов от угроз, классифицированных с учетом возможных нарушений безопасности защищаемых ресурсов. Рассматриваются все разновидности угроз, при этом наиболее опасные связаны с действиями субъектов–пользователей. На рис. 1 показаны основные компоненты безопасности РКС и их взаимосвязь.

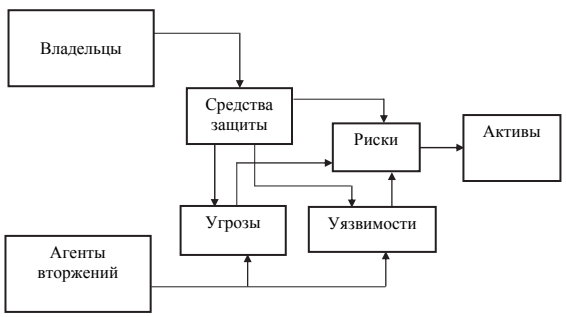

Рис. 1. Компоненты безопасности РКС и их взаимосвязь

Ответственность за безопасность защищаемых ресурсов возлагается на их владельцев, определяющих их ценность. Ресурсы представляют собой ценность также и для потенциальных агентов вторжений, которые пытаются получить несанкционированный доступ к ним. С точки зрения владельцев информации, угрозы безопасности представляют собой потенциальные воздействия на их ресурсы, приводящие, в том числе, к снижению их ценности. К типичным нарушениям безопасности относятся [1, 2]: потеря конфиденциальности ресурса путем несанкционированного доступа к нему с нанесением ущерба; потеря целостности ресурса вследствие несанкционированной модификации; потеря доступности вследствие некорректного лишения доступа к ресурсу легального субъекта.

В результате анализа существующих угроз определяются риски защищенности ресурсов РКС. Кроме того, данный анализ позволяет определить и выбрать контрмеры для нейтрализации потенциальных угроз и снизить риски защищенности до приемлемого уровня. Контрмеры снижают число потенциальных уязвимостей в РКС и поддерживают установленную в ней политику безопасности. При этом даже после реализации контрмер могут оставаться некоторые так называемые остаточные уязвимости, используемые агентами вторжений. Эти уязвимости формируют остаточный риск, снижаемый путем применения дополнительных средств защиты.

Перед тем, как предоставить доступ к своим ресурсам, их владельцы должны убедиться в том, что предпринятые контрмеры обеспечивают адекватное противостояние потенциальным угрозам. В общем случае, владельцы ресурсов не всегда могут оценить эффективность используемых средств защиты, тогда необходима независимая оценка. Результат такой оценки – степень доверия средствам защиты с учетом уменьшения рисков защищенности ресурсов. Степень доверия – характеристика средств защиты, подтверждающая корректность и эффективность их использования в конкретном случае. Данная оценка используется владельцем ресурсов в процессе принятия решения о допустимом уровне риска защищенности для его ресурсов. На рис. 2 показана взаимосвязь между степенью доверия к средствам защиты и уровнем риска защищенности ресурсов РКС.

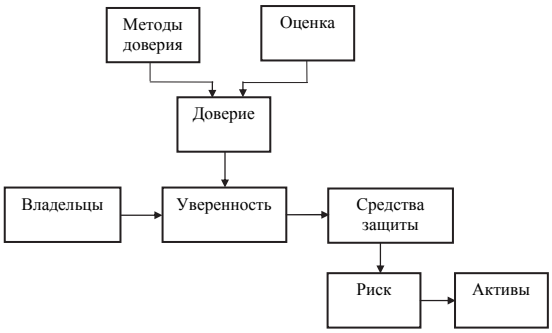

Рис. 2. Взаимосвязь понятий, используемых при оценке рисков защищенности

Результаты оценки параметров безопасности должны быть верифицированы с точки зрения их корректности, что позволит использовать данные оценки для обоснования допустимого уровня риска защищенности в конкретной среде РКС [3].

Формализованное представление модуля управления заданиями РКС на основе механизма *UML*-диаграмм

Важный компонент РКС – модуль управления заданиями (МУЗ), выполняющий функции по распределению решаемых заданий, в том числе заданий, связанных с управлением безопасностью РКС. Нарушение функционирования МУЗ, в частности задержки в анализе ситуаций и принятии решений по реакции на них, особенно в случае обработки критичной информации, потенциально приводит к нарушению или даже к полному прекращению работы РКС. Таким образом, существенный вопрос – анализ и снижение риска защищенности процесса функционирования МУЗ.

Выполним формализацию процесса анализа риска защищенности МУЗ на основе современных технологий разработки программного обеспечения.

На начальном этапе процесса анализа рисков защищенности на основе общей структурной схемы модуля управления заданиями РКС (рис. 3) [4, 5] формируются *UML*-диаграммы: прецедентов, развертывания и последовательности.

Диаграмма прецедентов отражает на верхнем уровне общую функциональность и параметры МУЗ, в том числе риск превышения допустимого времени анализа ситуаций и принятия решения, который связан с риском защищенности всей системы. Далее анализируемые параметры представляются на диаграмме последовательности, которая описывает последовательность действий, реализуемых при анализе ситуаций в РКС, с помощью специальных сообщений [6, 7].

Для модуля управления заданиями (*Control Tasks*) критичным есть риск превышения времени анализа ситуаций и принятия решений.

Для оценки данного риска администратор безопасности анализирует следующие параметры: граничное (критичное) время анализа си-

туаций и принятия решений (*limT*) и соответствующую ему причину превышения данного времени (*timeexcess.reason*), а также задает максимальное время, допустимое для принятия решения. На диаграмме прецедентов (рис. 4) задано максимальное время решения *lateTiming* – 30 с. Кроме того, оцениваются еще два параметра, влияющих на риск превышения времени принятия решения: вероятность (*timeexcess.probability*) и последствия (*timeexcess.consequence*) превышения времени решения. На рис. 4 данные параметры обозначены как *Prob* и *Cons*.

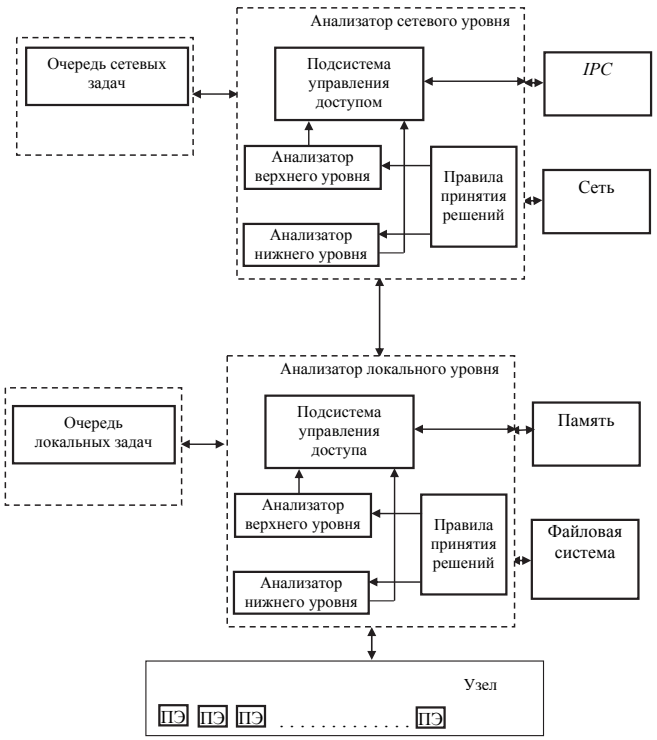

Рис. 3. Обобщенная схема модуля управления заданиями

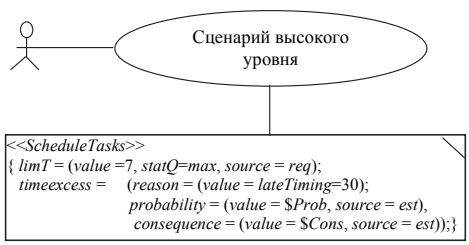

Рис. 4. Диаграмма прецедентов МУЗ

Входные параметры МУЗ определяются в диаграммах развертывания и последовательности, как показано на рис. 5 и 6. В качестве входных параметров выступают константы, переменные или выражения, описывающие формальную модель МУЗ.

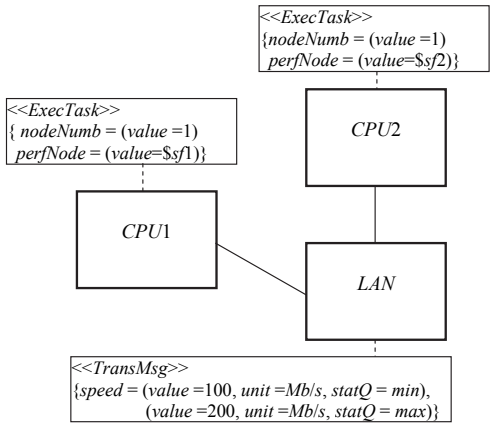

Рис. 5. Диаграмма развертывания МУЗ

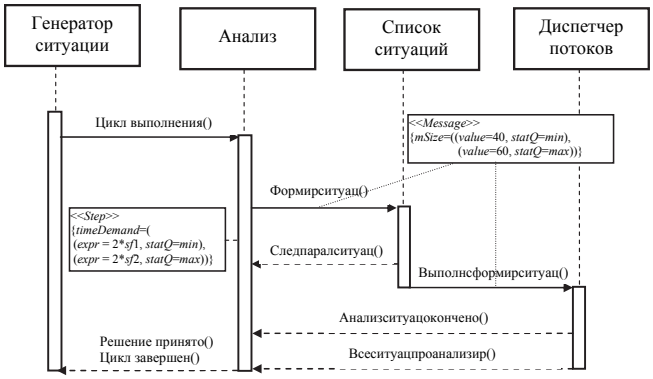

Рис. 6. Диаграмма последовательности МУЗ

Диаграмма развертывания (рис. 5) включает входные параметры, определяющие характеристики ресурсов РКС, такие как *nodeNumb*, *perfNode* и *speed*. Первый параметр определяет множество узлов РКС, второй – скорость обработки данных в узле в рассматриваемой системе, третий – скорость передачи сообщений, которая задается в виде граничного интервала от минимального до максимального значений. Данный параметр используется в дальнейшем при разработке модели Временной Сети Петри для МУЗ для установки времен срабатывания переходов, соответствующих передаче данных (сообщений) [8, 9].

Диаграмма последовательности включает следующие параметры: требования к времени анализа ситуации (*timeDemand*) и размер сообщения *Message* (*mSize*), определяющий объем информации, передаваемой в процессе взаимодействия между узлами МУЗ. Оба парамет-

ра представим в виде переменных, описывающих минимальное (*statQ* = min) и максимальное (*statQ* = max) допустимые значения.

Алгоритм работы МУЗ может быть реализован последовательно или параллельно в зависимости от требований к времени анализа ситуаций и принятия решений.

Оценка риска превышения времени анализа ситуаций и принятия решений

В рассматриваемом случае задача анализа рисков защищенности сводится к оценке риска превышения заданного времени анализа ситуаций и принятия решений в модуле управления заданиями РКС. Данный риск зависит от двух факторов: вероятности (*timeexcess.probability*) и последствий (*timeexcess.consequence*) осуществления события превышения времени принятия решения. Вероятность превышения заданного времени является функциональной зависимостью от времени анализа ситуаций и принятия решений, определенного в диаграмме прецедентов, а также от значений верхней и нижней границ допустимого интервала времени анализа ситуации и принятия решения.

Введем параметры α_i и β_j – число событий (в единицу времени), соответственно, реализации *i*-й угрозы безопасности и включения *j*-го канала средств защиты. Естественно, что на риски защищенности влияет интенсивность использования средств защиты, т.е. скорость реакции на те или иные опасные события. В том случае, если угрозы превысили возможности средств защиты, развивается атака на ресурсы. Также введем нормирующие коэффициенты $K_з$, K_a и параметр R_0 – начальный риск защищенности. При этом: $K_з$ – нормирующий коэффициент, определяющий степень эффективности мер (событий) защиты информации, K_a – нормирующий коэффициент, определяющий степень опасности угроз (событий) реализации НСД к информации.

Для оценки рисков защищенности РКС введем экспоненциальную функцию:

$$R_{ij}(t) = R_0 * e^{-(K_з*\beta_j - K_a*\alpha_i)*t}. \qquad (1)$$

Функция $R_{ij}(t)$ представляет собой риск реализации *i*-й угрозы для *j*-го канала защиты ценного ресурса в зависимости от времени *t*. Надежность S_{ij} средств защиты информации по предотвращению *i*-й угрозы по *j*-му каналу защиты определяется как:

$$S_{ij} = 1 - R_{ij}. \qquad (2)$$

Фактически, параметр S_{ij} представляет собой вероятность нереализации *i*-й угрозы по *j*-му каналу защиты.

Общий уровень надежности S_j по *j*-му каналу средств защиты РКС оценивается как:

$$S_j = \prod_{i=1}^{n} (1 - R_{ij}). \qquad (3)$$

В свою очередь риск защищенности R_j по всем угрозам безопасности РКС для *j*-го канала защиты равен:

$$R_j = 1 - S_j = 1 - \prod_{i=1}^{n} (1 - R_{ij}). \qquad (4)$$

В результате, общий риск защищенности *R* РКС по всем угрозам безопасности РКС и всем каналам защиты рассчитывается как:

$$R = 1 - \prod_{j=1}^{m} S_j = 1 - \prod_{j=1}^{m} \left(\prod_{i=1}^{n} (1 - R_{ij}) \right) \qquad (5)$$

или, в общем виде:

$$R(t) = 1 - \prod_{j=1}^{m} \left(\prod_{i=1}^{n} \left(1 - R_0 * e^{-\left(K_з*\beta_j - K_a*\alpha_i\right)*t} \right) \right), \qquad (6)$$

где *m* – число каналов защиты РКС, *n* – число угроз безопасности.

Возможны различные варианты развития ситуаций с точки зрения безопасности РКС, зависящие от соотношения между параметрами $K_a*\alpha_i$ и $K_з*\beta_j$. Если $K_a*\alpha_i > K_з*\beta_j$, то имеет место семейство процессов, отражающих ситуацию, когда риски защищенности растут и угрозы могут преобразоваться в реальную атаку. Наоборот, если $K_a*\alpha_i < K_з*\beta_j$, то имеет место снижение рисков защищенности и возможности реализации атак.

Проведем моделирование динамики процессов развития вторжений в зависимости от интенсивности событий, связанных с угрозами (α_i), интенсивности включения механизмов предотвращения вторжений (β_j), а также нормирующих коэффициентов $K_з$ и K_a.

По статистике [10] в современных компьютерных системах число попыток вторжений составляет в среднем 20 в сутки. Тогда для распределенной компьютерной системы, состоящей из 1000 узлов (рабочих станций), имеем оценку порядка 20000 попыток вторжений в сутки. Таким образом, математическое ожидание интенсивности реализации угроз безопасности в распределенной компьютерной системе оценивается как $\alpha_i = 0{,}25$, т.е. в среднем одна попытка вторжения за каждые четыре секунды.

Моделирование для оценки рисков защищенности R_{ij}, т.е. рисков реализации i-й угрозы для j-го канала защиты проведем для следующих исходных данных: эффективность средств защиты $K_з = 0{,}75$, степень опасности угроз $K_a = 0{,}8$. В первом случае зафиксируем интенсивность включения механизмов предотвращения вторжений на уровне $\beta = 0{,}4$, и построим семейство кривых для различных α_i ($\alpha_1 = 0{,}55$, $\alpha_2 = 0{,}6$, $\alpha_3 = 0{,}65$) при начальном риске $R_0 = 0{,}2$. Во втором случае зафиксируем интенсивность событий, связанных с реализацией угроз безопасности на уровне $\alpha = 0{,}3$, и построим семейство кривых для различных β_i ($\beta_1 = 0{,}3$, $\beta_2 = 0{,}35$, $\beta_3 = 0{,}4$) при начальном риске $R_0 = 1{,}0$. Полученные результаты представлены в табл. 1.

Т а б л и ц а 1

α, β	t, с	0	1	2	3	4	5	6	7	8	9	10
$\beta = 0{,}4$	$\alpha_1 = 0{,}55$	0,2	0,223	0,270	0,316	0,371	0,436	0,511	0,600	0,703	0,826	0,969
	$\alpha_2 = 0{,}6$	0,2	0,239	0,286	0,342	0,409	0,491	0,588	0,703	0,842	1,009	1,207
	$\alpha_3 = 0{,}65$	0,2	0,249	0,304	0,371	0,453	0,554	0,676	0,826	1,009	1,231	1,504
$\alpha = 0{,}3$	$\beta_3 = 0{,}3$	1,0	0,951	0,905	0,860	0,819	0,779	0,741	0,705	0,670	0,638	0,607
	$\beta_2 = 0{,}35$	1,0	0,928	0,861	0,800	0,741	0,688	0,638	0,592	0,549	0,510	0,472
	$\beta_1 = 0{,}4$	1,0	0,905	0,819	0,741	0,670	0,607	0,549	0,497	0,449	0,407	0,368

В соответствии с данными табл. 1, на рис. 7 и 8 представлена динамика процессов развития вторжений и изменения рисков защищенности R_{ij}.

Рис. 7 отражает рост рисков защищенности R_{ij} при фиксированном потоке событий предупреждения вторжений ($\beta = \text{const}$) в условиях динамической интенсивности угроз безопасности. Начальный уровень рисков угроз защищенности (R_0) установлен в значение 0,2. Далее, в процессе развития вторжений уровень рисков возрастает с различной скоростью (семейство кривых α_1, α_2, α_3) и достигает критичного уровня 0,8. Как видно из рис. 7, критичное время анализа ситуаций и принятия решений (время достижения уровня 0,8) зависит от интенсивности вторжений, и при высокой интенсивности ($\alpha_3 = 0{,}65$) может быть достигнуто достаточно быстро (примерно за 6,8 с). Фактически, критичное время определяет тот интервал времени, когда события, связанные с угрозами, еще не преобразуются в атаки.

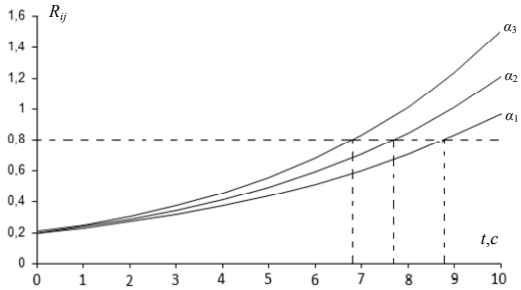

Рис. 7. Динамика изменения угроз безопасности и рисков защищенности

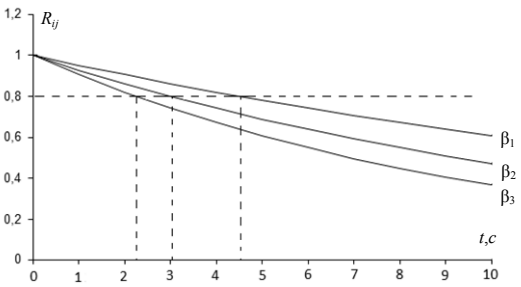

Рис. 8. Динамика изменения рисков защищенности и восстановления уровня защищенности

Вторая ситуация возникает в случае фиксированного потока событий угроз безопасности ($\alpha = \text{const}$) при включении различных механизмов (средств) предотвращения вторжений (рис. 8).

На рис. 8 установлен изначально высокий уровень рисков реализации угроз защищенности $R_0 = 1{,}0$, для его снижения требуется включить дополнительные средства защиты. Интенсивность включения средств защиты оказывается различной (семейство кривых). При этом (рис. 8), чем выше параметр β_j, тем быстрее достигается допустимый уровень рисков защищенности, который в данном случае установ-

лен на уровне 0,8. Так, для $\beta_j = 0{,}4$ уровень риска снижается до допустимого уже через 2,2 с.

В табл. 2 приведены значения критичных времен, полученных на основе зависимостей рис. 7 и 8.

Таблица 2

α, β		*t*, с
$\beta = 0{,}4$	$\alpha_1 = 0{,}55$	6,8
	$\alpha_2 = 0{,}6$	7,75
	$\alpha_3 = 0{,}65$	8,8
$\alpha = 0{,}3$	$\beta_3 = 0{,}3$	2,2
	$\beta_2 = 0{,}35$	3,0
	$\beta_1 = 0{,}4$	4,6

Таким образом, предложенные оценки рисков защищенности позволяют получить прогнозные значения критичного времени анализа ситуации и принятия решения в зависимости от интенсивности событий, связанных с угрозами безопасности, интенсивности включения механизмов предотвращения вторжений, а также от уровня эффективности средств защиты и степени опасности угроз безопасности.

Для анализа вероятности превышения критичного времени принятия решения, т.е. реакции средств защиты на угрозы, в условиях динамического изменения параметров безопасности РКС эффективным подходом представляется построение модели модуля управления заданиями с использованием специального аппарата моделирования на основе сетей.

Заключение. Анализ процессов в модуле управления заданиями РКС позволяет определить критичное время принятия решения по управлению безопасностью, а также оценить величину рисков защищенности. Предложенные аналитические оценки рисков защищенности позволяют комплексно проанализировать динамику процессов развития вторжений, процессов восстановления уровня защищенности и соответствующую динамику изменения уровня рисков защищенности РКС.

Для анализа вероятности превышения критичного времени реакции средств защиты на угрозы безопасности актуальна формализация представления процессов модуля управления заданиями РКС, в частности, на основе специальных сетевых механизмов и моделей, что позволит динамично оценить интервальные границы критичного времени реакции средств защиты на действия агентов вторжения.

1. *ISO*/*IEC* 15408-2009:1. Information technology – Security techniques – Evaluation criteria for IT security. Part1. – http://ebookbrowse.com/i/iso-15408-1-pdf
2. *Maiwald E.* Fundamentals of network security. – New York: McGraw-Hill. Technology Education, 2004. – 645 с.
3. *Мухин В.Е.* Инструментарий минимизации риска защищенности в распределенных компьютерных системах. // Системні дослідження та інформаційні технології. – 2010. – № 4. – С. 58–68.
4. *Job scheduling* in a heterogeneous GRID environment / H. Shan, W. Smith, L. Oliker et al. – 12 p. – http:// www.osti.gov/bridge/servlets/purl/860301-UfJBKm/860301.pdf
5. *Bowman I.* Conceptual Architecture of the Linux Kernel. – 13 p. – http://www.grad.math.uwaterloo.ca/~itbowman/CS746G/a1/
6. *Model-based* security analysis in seven steps. A guided tour to the CORAS method / Der F. Braber, I. Hoggavink, M. Lund et al. // BT Technology, 2007. – **1**, N 25. – P. 101–117.
7. *Ober I.*, *Graf S.* Validating timed UML models by simulation and verification. // Intern. J. «Software tools for Technology», 2006. – **8**, N 2. – P. 128–145.
8. *Vicario E.* Static analysis and dynamic steering of time-dependent systems. // IEEE Trans. on Software Engineering, 2001. – **27**, N 8. – P. 728–748.
9. *Vicario E.*, *Sassoli L.*, *Carnevali L.* Using stochastic state classes in quantitative evaluation of dense-time reactive reactive systems // IEEE Trans. on Software Engineering, 2009. – **35**, N 5. – P. 703–719.
10. *CERT*/*CC* Statistics 2001–2008. Yearly CERT publication. – http://www.cert.org

Поступила 04.07.2011

Тел. для справок: (044) 406-8650, (067) 508-7684 (Киев)
E-mail: *mukhin@comsys.ntu-kpi.kiev.ua*