УДК 004.3

В.В. Анищенко, Л.И. Кульбак

ОЦЕНКА УЩЕРБА РАБОТОСПОСОБНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Предлагается ввести оценку ущерба информационной безопасности от потери работоспособности информационной системы (объекта). В качестве показателя наносимого ущерба рассчитывается коэффициент возможной (потенциальной) доступности. Показатель доступности определяется методами теории надежности.

Введение

Под безопасностью информации, или информационной безопасностью, принято понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей ее структуре [1].

Не вызывает сомнения, что потеря работоспособности информационной системы наносит ущерб как владельцам, так и пользователям информации. Под работоспособным состоянием (РС) в соответствии с ГОСТ 27.002 [2] следует понимать состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и (или) конструкторской (проектной) документации.

Условимся считать, что РС информационной системы обеспечивает возможный доступ пользователей к ее информации. В этом случае наглядным показателем работоспособности объекта может быть доля календарного времени РС объекта. Примем ее в качестве показателя возможной доступности пользователей к информации. Назовем долю календарного времени РС объекта коэффициентом возможной (потенциальной) доступности.

Можно показать, что при условии непрерывной работы комплексный показатель надежности – коэффициент готовности – численно равен коэффициенту возможной доступности.

Согласно [3] коэффициент готовности – это вероятность того, что объект окажется в РС в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается.

Календарное время использования объекта можно представить в виде сумм отрезков: времени РС объекта при его использовании по назначению, времени неработоспособного состояния (НРС) при использовании объекта по назначению и времени неиспользования объекта по назначению.

Статистически коэффициент возможной доступности и коэффициент готовности следует определять по формуле [4]

$$K_{\text{ВД}} = \frac{T_{\text{РС}}(t_{\text{К}})}{t_{\text{К}}} = K_{\text{Г}}, \qquad (1)$$

где $K_{\text{ВД}}$ – коэффициент возможной доступности;

$T_{\text{РС}}(t_{\text{К}})$ – суммарное время РС системы (объекта) в интервале календарного времени $t_{\text{К}}$;

$t_{\text{К}}$ – интервал календарного времени;

$K_{\text{Г}}$ – коэффициент готовности.

Это выражение позволяет для оценки показателя возможной доступности системы (объекта) использовать методы теории и практики надежности.

Рассмотрим риск, связанный с потенциальной доступностью. Согласно СТБ ИСО/МЭК. Руководство 73–2005 [5] риск – это комбинация вероятности наступления вреда и тяжести последствий вреда. В качестве вреда от потери доступности к информации можно

принять потери времени, а в качестве вероятности этого события – вероятность недоступности к информации.

В качестве показателя ущерба можно дополнительно принять суммарное время НРС объекта в течение одного года. Этот показатель связан с коэффициентом возможной доступности формулой

$$t_{\text{НР}} = 525\,600(1 - K_{\text{ВД}}), \tag{2}$$

где $t_{\text{НР}}$ – суммарное время НРС объекта в течение одного года, мин; 525 600 – количество минут в году.

1. Методология оценки коэффициента возможной доступности

Расчет коэффициента доступности информационной системы (объекта) следует начинать с составления структурной схемы доступности (ССД). ССД объекта можно всегда свести к последовательному соединению элементов ССД, которое отражает потерю работоспособности объекта при отказе хотя бы одного элемента (рис. 1). В качестве элементов схемы (ЭС) используются отдельные технические средства (ТС) и группы ТС, имеющие резерв.

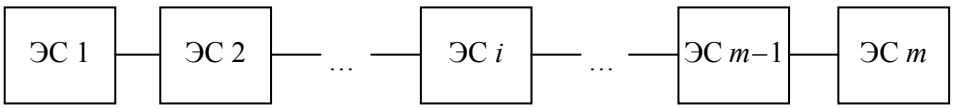

Рис. 1. Типовая ССД объекта

В соответствии с ССД на рис. 1 коэффициент возможной доступности объекта следует вычислять по формуле

$$K_{\text{ВД.ОБ}} = \prod_{i=1}^{m} K_{\text{ВД}.i}\ , \tag{3}$$

где $K_{\text{ВД.ОБ}}$ – коэффициент возможной доступности объекта;

$K_{\text{ВД}.i}$ – коэффициент возможной доступности i-го ЭС объекта;

m – количество ЭС в ССД объекта.

Среди ЭС объекта будем различать простые и сложные ЭС. Простые ЭС объекта – это отдельные ТС, не имеющие в своем составе резервных ТС. Сложные ЭС объекта – это группа ТС, имеющая в своем составе резервные элементы.

2. Расчет коэффициентов возможной доступности ЭС ССД

Любой ЭС в процессе эксплуатации находится в множестве состояний. Состояние ЭС зависит от состояния ее составных частей (СЧ). Состояние СЧ со временем изменяется, и, следовательно, появляется большое число вариантов состояний ЭС за счет комбинации состояний СЧ.

Пусть имеют место следующие допущения [6]:

– ЭС состоит из определенного количества недекомпозируемых элементов ЭС;

– ЭС может находиться в одном из двух состояний: РС или НРС;

– события, переводящие ЭС из одного состояния в другое, случайные и независимые с известными постоянными значениями интенсивности события;

– переход ЭС из одного состояния в другое совершается независимо от предыдущих переходов;

– за исходное состояние ЭС принимается состояние, при котором все элементы ЭС работоспособны.

Модель состояний ЭС принято наглядно представлять в виде размеченного графа. Узлами графа являются состояния, а ребрами со стрелками – пути перехода из одного состояния в

другое. У каждого ребра графа проставляется интенсивность перехода $\lambda_{i.j}$, где i – номер узла, из которого выполняется переход; j – номер узла, куда выполняется переход.

Пусть множество состояний ЭС W разделяется на два непересекающихся подмножества: подмножество РС $W_{\text{РС}}$ и подмножество НРС $W_{\text{НРС}}$. В подмножестве $W_{\text{РС}}$ выделим подмножество состояний, из которых возможен непосредственный переход в подмножество $W_{\text{НРС}}$, и обозначим его $W_{\text{РС–НРС}}$. В подмножестве $W_{\text{НРС}}$ выделим подмножество состояний, из которых возможен непосредственный переход в подмножество $W_{\text{РС}}$, и обозначим его $W_{\text{НРС–РС}}$.

Коэффициент возможной доступности $K_{\text{ВД}}$ по определению равен вероятности пребывания ЭС в произвольный момент времени в РС. Следовательно, его следует определять по формуле

$$K_{\text{ВД. ЭС}} = \sum_{j \in W_{\text{РС}}} P_j, \tag{4}$$

где P_j – вероятность пребывания ЭС в состоянии j подмножества $W_{\text{РС}}$.

Для определения вероятностей состояний ЭС, которые фигурируют в формуле (4), строится размеченный граф состояний ЭС, по которому записывается система алгебраических уравнений. При составлении системы уравнений предлагается пользоваться мнемоническим модифицированным правилом [7].

Каждому состоянию (узлу) графа соответствует уравнение. В правой части уравнения записывается произведение вероятности данного состояния и суммы интенсивностей, расставленных на стрелках, выходящих из данного состояния. В левой части уравнения записывается сумма произведений интенсивности перехода по этим стрелкам в рассматриваемое состояние и вероятности состояния, откуда осуществлялся переход. Число членов в правой части уравнения равно числу стрелок, направленных в данное состояние.

Число уравнений должно равняться числу состояний на графе. Из системы уравнений исключается одно из уравнений и вместо него добавляется уравнение нормировки

$$\sum_{j \in W} P_j = 1. \tag{5}$$

Система алгебраических уравнений решается одним из известных способов, а результаты решения подставляются в формулу (4).

Получим формулы для расчета коэффициента доступности ЭС различной структуры.

В нормативной документации по надежности, как правило, принято считать, что наработка на отказ элемента информационной системы имеет экспоненциальный закон распределения. Такой же закон распределения принимается и для времени восстановления.

Простой ЭС (рис. 2) может находиться в одном из двух состояний: РС или НРС. На рис. 2 приняты следующие обозначения:

S_0 – исходное РС ЭС;

S_1 – НРС ЭС;

λ – интенсивность отказов ЭС;

V – интенсивность восстановления ЭС.

Здесь $\lambda = 1/T_{\text{О}}$; (6)

$V = 1/T_{\text{В}}$, (7)

где $T_{\text{О}}$ – средняя наработка на отказ ЭС;

$T_{\text{В}}$ – среднее время восстановления ЭС.

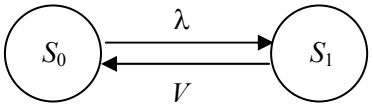

Рис. 2. Граф состояний простого ЭС

Таким образом, согласно графу на рис. 2 система уравнений примет следующий вид:

$$\begin{cases} \lambda P_0 = V P_1; \\ \mathrm{P}_0 + P_1 = 1. \end{cases}$$

Корнями этой системы уравнений являются

$$P_0 = \frac{V}{V+\lambda}; \tag{8}$$

$$P_1 = \frac{\lambda}{V+\lambda}. \tag{9}$$

В соответствии с формулой (4) получим

$$K_{\text{ВД.ЭС}} = \frac{V}{V+\lambda} = \frac{T_{\text{О}}}{T_{\text{О}} + T_{\text{В}}}. \tag{10}$$

Сложный ЭС (например, дублирование) изображен на рис. 3.

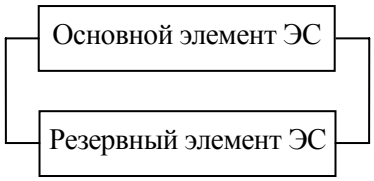

Рис. 3. ССД ЭС с однократным резервированием (дублированием)

Граф состояний резервированного ЭС в случае недостоверной реконфигурации ЭС при отказе резервного элемента ЭС показан на рис. 4.

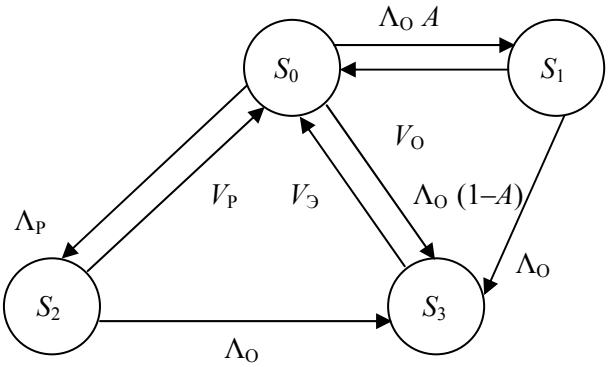

Рис. 4. Граф состояний резервированного ЭС при недостоверной реконфигурации

На рис. 4 приняты следующие обозначения:

S_0 – исходное состояние ЭС (основной и резервный элементы ЭС работоспособны): ЭС работоспособен;

S_1 – отказал основной элемент ЭС и реконфигурация прошла успешно: ЭС работоспособен;

S_2 – отказал резервный элемент: ЭС работоспособен;

S_3 – отказал основной элемент ЭС и реконфигурация не прошла успешно: ЭС неработоспособен;

$\Lambda_{\text{О}}$ – интенсивность отказов основного элемента ЭС;

$\Lambda_{\text{Р}}$ – интенсивность отказов резервного элемента ЭС;

A – вероятность успешной реконфигурации;

$V_{\text{О}}$ – интенсивность восстановления основного элемента ЭС в обычном случае;

$V_{\text{Э}}$ – интенсивность восстановления основного элемента ЭС в экстренном случае (когда отказали оба элемента ЭС);

$V_{\text{Р}}$ – интенсивность восстановления резервного элемента ЭС.

При принятых ранее допущениях справедливы следующие соотношения:

$$\Lambda_{\text{О}} = 1/T_{\text{О}}\,, \tag{11}$$

где $T_{\text{О}}$ – средняя наработка на отказ основного элемента ЭС;

$$\Lambda_{\text{Р}} = 1/T_{\text{О.Р}}\,, \tag{12}$$

где $T_{\text{О.Р}}$ – средняя наработка на отказ резервного элемента ЭС;

$$V_{\text{О}} = 1/T_{\text{В.О}}\,, \tag{13}$$

где $T_{\text{В.О}}$ – среднее время восстановления основного резервированного элемента ЭС в обычном случае;

$$V_{\text{Э}} = 1/T_{\text{В.Э}}\,, \tag{14}$$

где $T_{\text{В.Э}}$ – среднее время восстановления основного резервного элемента ЭС в экстренном случае;

$$V_{\text{Р}} = 1/T_{\text{В.Р}}\,, \tag{15}$$

где $T_{\text{В.Р}}$ – среднее время восстановления резервированного элемента ЭС.

Система уравнений в соответствии с вышеизложенным примет следующий вид:

$$\begin{gathered}(\Lambda_{\text{О}} + \Lambda_{\text{Р}})P_0 = V_{\text{О}}P_1 + V_{\text{Р}}P_2 + V_{\text{Э}}P_3;\\ (V_{\text{О}} + \Lambda_{\text{О}})P_1 = \Lambda_{\text{О}}\,AP_0;\\ (V_{\text{Р}} + \Lambda_{\text{О}})P_2 = \Lambda_{\text{Р}}\,P_0;\\ P_0 + P_1 + P_2 + P_3 = 1.\end{gathered} \tag{16}$$

Корнями системы уравнений (16) являются

$$P_1 = \frac{\Lambda_{\text{О}}A}{(V_{\text{О}} + \Lambda_{\text{О}})}P_0; \tag{17}$$

$$P_2 = \frac{\Lambda_{\text{Р}}}{(V_{\text{Р}} + \Lambda_{\text{О}})}P_0; \tag{18}$$

$$P_3 = \frac{\Lambda_{\text{О}}}{V_{\text{Э}}}(P_1 + P_2) + \frac{\Lambda_{\text{О}}(1-A)}{V_{\text{Э}}}P_0; \tag{19}$$

$$P_0 = [1 + \frac{\Lambda_{\text{О}}(1-A)}{V_{\text{Э}}} + (1 + \frac{\Lambda_{\text{О}}}{V_{\text{Э}}})(\frac{\Lambda_{\text{О}}A}{V_{\text{О}} + \Lambda_{\text{О}}} + \frac{\Lambda_{\text{Р}}}{V_{\text{О}} + \Lambda_{\text{Р}}})]^{-1}. \tag{20}$$

Приведем обозначения, принятые в формуле (4), для графа на рис. 4: $0, 1, 2, 3 \in W$, $0, 1, 2 \in W_{\text{РС}}$, $\Lambda_{0.1} = \Lambda_{\text{О}}A$, $\Lambda_{1.0} = V_{\text{О}}$, $\Lambda_{0.2} = \Lambda_{\text{Р}}$, $\Lambda_{0.3} = \Lambda_{\text{О}}(1-A)$, $\Lambda_{2.0} = V_{\text{Р}}$, $\Lambda_{3.0} = V_{\text{Э}}$, $\Lambda_{2.3} = \Lambda_{\text{О}}$, $\Lambda_{1.3} = \Lambda_{\text{О}}$.

В соответствии с формулой (4)

$$K_{\text{ВД. ЭС}} = P_0 + P_1 + P_2. \tag{21}$$

После подстановки в формулу (21) формул (17), (18) и (20) получим

$$K_{\text{ВД.Р.ЭС}} = \frac{1 + B_{\text{О}} + B_{\text{Р}}}{1 + \Lambda_{\text{О}}(1 - A)T_{\text{В.Э}} + (1 + \Lambda_{\text{О}})T_{\text{В.Э}}(B_{\text{О}} + B_{\text{Р}})}; \tag{22}$$

$$B_{\text{О}} = \frac{\Lambda_{\text{О}} A T_{\text{В.О}}}{1 + \Lambda_{\text{О}} T_{\text{В.О}}}; \tag{23}$$

$$B_{\text{Р}} = \frac{\Lambda_{\text{Р}} T_{\text{В.Р}}}{1 + \Lambda_{\text{О}} T_{\text{В.Р}}}, \tag{24}$$

где $K_{\text{ВД.Р.ЭС}}$ – коэффициент возможной доступности резервированного ЭС.

Дробное (скользящее) резервирование ЭС изображено на рис. 5.

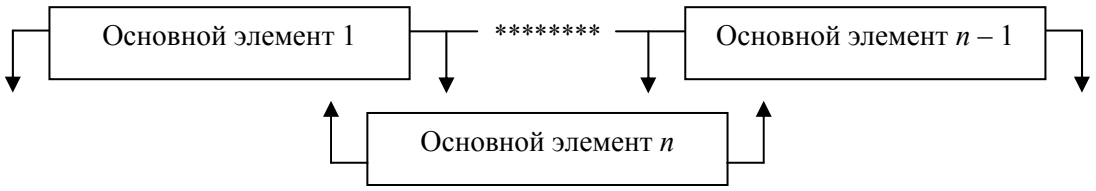

Рис. 5. ССД ЭС с дробным резервированием 1/*n* (со скользящим резервом)

Граф состояний резервного ЭС в случае достоверной реконфигурации СЧ при отказе резервных элементов ЭС и при дробном резервировании изображен на рис. 6.

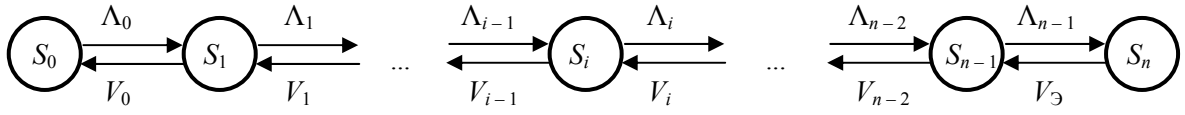

Рис. 6. Граф состояний резервированного ЭС

На рис. 6 приняты следующие обозначения:

S_0 – исходное состояние ЭС, когда все n элементов ЭС работоспособны;

S_i – состояние ЭС, когда отказали i из n элементов ЭС;

S_n – состояние ЭС, когда отказали все n элементов СЧ (предельное число отказавших элементов: ЭС неработоспособно);

Λ_i, $i = 0, ..., n - 1$, – интенсивность перехода ЭС из состояния S_i в состояние S_{i+1};

V_i, $i = 0, ..., n - 2$, – интенсивность перехода ЭС из состояния S_{i+1} в состояние S_i;

$V_{\text{Э}}$ – интенсивность перехода ЭС из состояния S_n в состояние S_{n-1};

n – предельное число отказавших ЭС.

В соответствии с правилами составления системы алгебраических уравнений по размеченному графу состояний, изложенными выше, и с учетом замены одного уравнения системы уравнений на уравнение нормировки система уравнений примет следующий вид:

$$\Lambda_0 P_0 = V_0 P_1;$$

$$(V_{i-1} + \Lambda_i) P_i = \Lambda_{i-1} P_{i-1} + V_i P_{i+1},\ i = 1, ..., n - 2; \tag{25}$$

$$(V_{n-2} + \Lambda_{n-1\,1})P_i = \Lambda_{n-2\,2}P_{n-2} + V_Э P_n,\ i = 1, ..., n-2;$$

$$\sum_{i=0}^{n} P_i = 1,$$

где P_i – вероятность пребывания ЭС в состоянии S_i.

Корнями системы уравнений (25) являются

$$P_0 = [1 + \frac{\Lambda_{n-1}}{V_Э}\prod_{j=0}^{n-2}\frac{\Lambda_j}{V_j}]^{-1}; \tag{26}$$

$$P_i = P_0\prod_{j=0}^{i-1}\frac{\Lambda_j}{V_j},\quad i = 1, ..., n-1; \tag{27}$$

$$P_n = P_0\frac{\Lambda_{n-1}}{V_Э}\prod_{j=0}^{i-1}\frac{\Lambda_j}{V_j}. \tag{28}$$

Для ЭС справедливо соотношение

$$\Lambda_i = (n-i)\Lambda,\ \ i = 0, ..., n-1, \tag{29}$$

где Λ – интенсивность отказов ЭС;

i – количество накопившихся отказавших ЭС.

При неограниченном восстановлении ЭС выполняются следующие условия:

$$V_i = (i+1)V,\ \ i = 0, ..., n-2,\ V_Э > nV, \tag{30}$$

где V – интенсивность восстановления отказавшего ЭС;

i – количество накопившихся отказавших ЭС;

$V_Э$ – интенсивность экстренного восстановления отказавшего ЭС.

С учетом соотношений (29), (30) и формул (26)–(28) получим

$$K^*_{\text{ВД.Р.ЭС}} = P_0(1 + \sum_{i=1}^{n-1} A^i\frac{n!}{(n-i)!i!}), \tag{31}$$

где

$$P_0 = [1 + \sum_{i=1}^{n-1} A^j\frac{n!}{(n-i)!\times i!} + \frac{VA^n}{V_Э}]^{-1}. \tag{32}$$

3. Пример расчета

Произведем расчет доступности в системе высокой готовности, выполненной в виде кластера [8, 9].

Кластер состоит из двух узлов (серверов), связанных между собой внутренней сетью, которая обеспечивает обмен сигналами активности. Узлы подключены к общему дисковому массиву (RAID-массиву) и к внешней локальной сети. Все подсистемы кластера имеют резервирование, поэтому при отказе любого элемента кластер в целом останется в РС. Более того, замена отказавшего элемента возможна без остановки кластера. На обоих узлах кластера устанавливается операционная система Microsoft Windows Server 2003 Enterprise, которая поддерживает технологию Microsoft Windows Cluster Service (MSCS).

Принцип работы кластера следующий. Приложение (служба), доступность которого обеспечивается кластером, устанавливается на обоих узлах. Для этого приложения создается группа ресурсов, включающая IP-адрес и сетевое имя виртуального сервера, а также один или несколько логических дисков на общем дисковом массиве. Таким образом, приложение вместе со своей группой ресурсов не привязывается жестко к конкретному узлу, а напротив, может

быть запущено на любом из этих узлов (при этом на каждом узле одновременно может работать несколько приложений).

Описанной системе соответствует ССД (рис. 7).

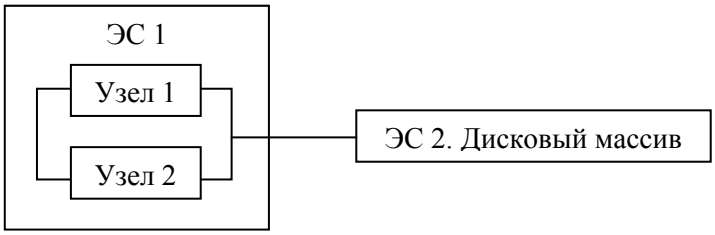

Рис. 7. ССД кластера

Примем следующие значения показателей надежности компонент кластера:
– средняя наработка на отказ узла (сервера) $T_{О.С} = 65\,000$ ч;
– среднее время восстановления узла (сервера) в обычном случае $T_{В.О.С} = 8$ ч;
– среднее время восстановления узла (сервера) в экстренном случае $T_{В.Э.С} = 2$ ч;
– вероятность перехода на резерв $A = 1{,}0$;
– средняя наработка на отказ дискового массива $T_{О.Д} = 100\,000$ ч;
– среднее время восстановления дискового массива $T_{ВД} = 4$ ч.

В соответствии с формулой (4)

$$K_{ВД.К} = K_{ВД.1} K_{ВД.2}, \tag{33}$$

где $K_{ВД.К}$ – коэффициент возможной доступности кластера;
$K_{ВД.1}$ – коэффициент возможной доступности ЭС 1;
$K_{ВД.2}$ – коэффициент возможной доступности ЭС 2.

ЭС 1 является непростым элементом ССД, и расчет показателя $K_{ВД.1}$ следует проводить по формулам (11), (12), (14), (22)–(24). В результате расчета $K_{ВД.1} = 0{,}999805$. ЭС 2 является простым элементом ССД и в результате расчета по формуле (10) $K_{ВД.2} = 0{,}999960$. В результате расчета по формуле (33) $K_{ВД.К} = 0{,}999764$.

Суммарное время НРС объекта в течение одного года, вычисленное по формуле (2), составило 124 мин.

Заключение

В работе обосновывается целесообразность ввода в нормативную документацию по информационной безопасности риска в виде коэффициента возможной (потенциальной) доступности и ущерба от недоступности в виде суммарного времени НРС объекта в течение одного года.

Введение такого рода риска в нормативную документацию будет способствовать повышению качества разработки информационных систем в части надежности.

Предлагается методология для расчета риска, которая иллюстрируется примером.

Список литературы

1. Информационные технологии безопасности и защиты [Электронный ресурс]. – 2012. – Режим доступа : http//inftis.narod.ru/it/5-6/n5.htm. – Дата доступа : 13.03.2012.

2. Доступность информации // Википедия [Электронный ресурс]. – 2012. – Режим доступа : http://ru.wikipedia.org. – Дата доступа : 13.03.2012.

3. Надежность в технике. Основные понятия. Термины и определения : ГОСТ 27.002–89. – М. : Изд-во стандартов, 1990. – 37 с.

4. Половко, А.М. Основы теории надежности / А.М. Половко, С.В. Гуров. – СПб. : БХВ-Петербург, 2006. – 620 с.

5. Менеджмент риска. Термины и определения. СТБ ИСО/МЭК Руководство 73–2005. – Минск : Госстандарт, 2005. – 12 с.

6. Анищенко, В.В. Надежность и отказоустойчивость кластерных вычислительных систем / В.В. Анищенко, Л.И. Кульбак, В.К. Фисенко // Автоматика и вычислительная техника. – 2004. – № 5. – С. 32–42.

7. Овчаров, Л.А. Прикладные задачи теории массового обслуживания / Л.А. Овчаров. – М. : Машиностроение, 1969. – 324 с.

8. Сравнение кластера надежности и «обычного» сервера. Компания «Тим Компьютерс» [Электронный ресурс]. – 2012. – Режим доступа : http://www.team.ru/server/stbl_compare.shtml. – Дата доступа : 13.03.2012.

9. Анищенко, В.В. Модели надежности кластерных вычислительных систем / В.В. Анищенко, Л.И. Кульбак, Т.С. Мартинович // Известия НАН Беларуси. Сер. физ.-техн. наук. – 2008. – № 1. – С. 89–99.

Поступила 13.03.12

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова,6
e-mail: lkulbak@yandex.ru

U.V. Anishchanka, L.I. Kulbak

ASSESSMENT OF LOSS OF INFORMATION SYSTEM PROCESSING CAPABILITY

It is proposed to introduce an assessment of information security damage from processing capability loss of an information system (object). As an indicator of damage it is proposed to use a coefficient of possible (potential). The indicator is determined by the reliability theory methods.