DOI: 10.7256/2073-8560.2013.6.9585



Царегородцев А. В., Ермошкин Г. Н.

# МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

***Аннотация.*** *Являясь одной из самых привлекательных современных информационных технологий, облачные сервисы могут, как оптимизировать процессы управления информационной безопасностью, так и усложнить для организации контроль над критичными данными и соблюдением контрмер на инциденты безопасности.Решение проблемы своевременного и качественного анализа рисков аутсорсинга информационной безопасности систем облачной архитектуры позволит решить множество проблем связанных с защитой от угроз использования информационных и телекоммуникационных технологий в противоправных целях. Широкое распространение и применение облачных вычислений диктует необходимость адаптации и доработки существующих моделей оценки рисков информационных систем. Подход, предлагаемый в статье, может быть использован для оценки рисков информационных систем, функционирующих на основе технологии облачных вычислений, и оценки эффективности принимаемых мер безопасности. При этом, оценка риска включает этапы анализа и оценивания, а анализ риска, в свою очередь, включает идентификацию и количественную оценку риска. Обеспечение оценки производится на основе определения контекста риска (выбора критериев риска и определения границ анализа). Под количественной оценкой риска понимается процесс моделирования, включающий разработку и анализ альтернативных сценариев риска, построение функций риска и определение вероятности его наступления.*

***Ключевые слова:*** *информационная безопасность, облачные вычисления, публичное облако, частное облако, гибридное облако, оценка риска, риск-модель, матрица воздействий, матрица потерь, матрица зависимости.*

## Введение

Являясь одной из самых привлекательных современных информационных технологий, облачные сервисы могут, как оптимизировать процессы управления информационной безопасностью, так и усложнить для организации контроль над критичными данными и соблюдением контрмер на инциденты безопасности.

Решение проблемы своевременного и качественного анализа рисков аутсорсин-

DOI: 10.7256/2073-8560.2013.6.9585



га информационной безопасности систем облачной архитектуры позволит решить множество проблем связанных с защитой от угроз использования информационных и телекоммуникационных технологий в противоправных целях.

Анализ существующих моделей оценки риска является основой для разработки новой модели на современном наборе стандартов с учетом особенностей национальной специфики необходимой для создания концепции обеспечения ИБ при заключении договора аутсорсинга и для поддержания уровня риска на приемлемом уровне.

Оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение ИБ и получаемую от них отдачу (в виде снижения суммарного риска). Поэтому более предпочтительными представляются количественные методики. Но они требуют наличия оценок вероятности возникновения для каждой из рассматриваемых угроз безопасности. Кроме того, использование интегральных показателей, таких как ALE, опасно тем, что неправильная оценка вероятности угрозы в отношении очень дорогостоящего актива может кардинально изменить оцениваемое значение суммарной стоимости рисков.

В работе представлен анализ теоретических и научно-практических методов оценки риска для сложных технических систем. При этом, оценка риска включает этапы анализа и оценивания, аанализ риска, в свою очередь, включает идентификацию и количественную оценку риска. Обеспечение оценки производится на основе определения контекста риска (выбора критериев риска и определения границ анализа). Под количественной оценкой риска будем понимать процесс моделирования, включающий разработку и анализ альтернативных сценариев риска, построение функций риска и определение вероятности его наступления.

## 1. Определение зависимостей и атрибутов безопасности

Большинство проблем с безопасностью, так или иначе, связанно с вредоносным воздействием. Проблема здесь в первую очередь связанна с невозможностью верно измерить все факторы, а если нельзя все верно рассчитать, то и управлять результатом не получится.

Таким образом, первостепенной задачей становится создание инструментария для ведения правильных и своевременных расчетов. Вычислив все возможные ошибки и потери системы от них мы получим возможность провести расчеты необходимых контрмер и оценить результат их применения.

Существует ряд моделей подходящих для решения данной задачи. В этих моделях для определения надежности системы используютсяследующие показатели:

- ***Наработка на отказ (MTTF)*** — это продолжительность работы системы до момента появления первого сбоя. Данный параметр измеряется как: количество часов работы без сбоя всех устройств деленное на количество устройств.
- ***Среднее время между отказами (MTBF)*** — описывает среднее время работы системы между двумя последовательными сбоями (применяется для систем подлежащих восстановлению). Измеряется как все время работы системы, в часах разделенное на количество отказов.
- ***Наработка до обнаружения (MTTD)*** — описывает время между обнаружением ранее неизвестных уязвимостей системы.
- ***Наработка до отказа (MTTE)*** — отражает время работы системы до момента возникновения ошибки или использования уязвимости известные ранее.

DOI: 10.7256/2073-8560.2013.6.9585



- ***Среднее доступное время работы*** — показатель времени в процессе работы системы, когда она доступна для использования.

Эти модели в том или ином виде отражают вероятность отказа всей системы, игнорируя различные особенности и начальное состояние систем, в т. ч. неравномерное распределение угроз, разницу в условиях возникновения ошибок и т. д.

В тоже время, например для оценки наработки системы на отказ, необходимо лишь смоделировать вероятности ошибок в соответствии с их спецификациями.

Чтобы использовать данные модели для решения задачи анализа рисков аутсорсинга информационной безопасности систем облачной архитектуры следует учесть следующие факторы:

- разницу в стоимости ошибки в зависимости от условия возникновения;
- разницу в вероятности возникновения сбоя для разных компонентов системы;
- разницу в результате возникновения ошибки для заинтересованных сторон.

В данной статье предлагается модель, в которой мы постарались учестьвсе вышеперечисленные факторы. Применение данной модели может способствовать рационализации принятия решений в системах облачных вычислений, тем самым способствовать сокращению издержек пользователей.

## 2. Модель оценки рисков

Распределенные информационно-вычислительные системы характеризуются пятью фундаментальными свойствами: функциональностью, мощностью, доступностью, стоимостью, надежностью. При этом, надежность будет включать и угрозы, и атрибуты, и средства её достижения.Несмотря на то, что существует ряд моделей позволяющих оценить надежность системы по таким показателям, как MTTF для выяснения отказоустойчивостии, MTTE для измерения уязвимостей системы, не существует способа измерить надежность напрямую или дать количественную оценку рискам безопасности.

Но, как показывает практика, не всегда возможно и нужно стараться учесть все существующие разновидности рисков. Так в большинстве случаев достаточно учитывать лишь риски, имеющие финансовую составляющую. Для их оценки в большей степени подходят количественные методы оценки.

В этом контексте предлагаемыйподход обладает рядом преимуществ:

- предлагаются данные о цене потерь: измеряя цену как количество финансовых потерь на единицу времени работы системы;
- проводятся измерения результатов ошибок: предоставляя количественный результат (цену) ошибок безопасности;
- предоставляются данные о потерях рассчитанные для различных заинтересованных сторон.

***Матрица потерь***

Пусть $S$ — система, а $H_1, H_2. \ldots, H_k$ заинтересованные стороны. $R_1, R_2, \ldots, R_n$ требования безопасности в системе. $ST_{i,\,j}$, где $1 \le i \le k$, $1 \le j \le n$, стоимость потерь для стороны $H_i$ в результате невыполнения требований безопасности $R_j$ в зависимости от сегмента распределенной архитектуры, находящегося в управлении заинтересованной стороны $H_i$. $PR_j$ где $1 \le j \le n$, вероятность, что система не соотносится с требованиями безопасности $R_j$, и $MFC_i$ где $1 \le i \le k$ переменная отражающая стоимость потерь для стороны $H_i$ в случае нарушения безопасности. Величина $MFC$ измеряется в финансовых потерях на единицу операционного времени:

$$MFC_i = \sum_{1 \le j \le n} ST_{i,j} * PR_j.$$

DOI: 10.7256/2073-8560.2013.6.9585



Пусть *MFC* вектор размерности *k* представляющий основные издержки в случаи нарушения требований безопасности, *PR* вектор размера *n* вероятность невыполнения требований безопасности и *ST* матрица $k \times n$ отражающая стоимость потерь в результате невыполнения требований безопасности, тогдаможно записать как произведение матриц:

$MFC = ST * PR$.

***Матрица зависимостей***

Пусть $C_1$, $C_2$, …, $C_n$ — компоненты системы *S*. В зависимости от того какие из этих элементов функционируют будут выполнятся или не выполнятся требования безопасности. Если предположить, что возможен отказ лишь одного компонента системы, тогда можно ввести следующие события:

- $E_i$ — событие при котором компонент $C_i$ перестал функционировать в результате нарушения безопасности ($1 \le i \le h$).
- $E_{m+i}$ — не один из компонентов не затронут.

Определив набор событий $E_i$можно записать вероятность наступления события *F* как: $P(F) = \sum_{k=1}^{h+1} P(F|E_k) * P(E_k)$.

Считаем что *F* — это событие, при котором не выполняется условие *R*, тогда:

$PR_j = \sum_{j=1}^{m+1} P(F_j|E_k) * P(E_k)$.

Здесь *DP*– матрица размерности$n \times h + 1$ , строки *j* и столбцы *k* отражают вероятность отказа системы в случае, если компонент *k* не выполнил требование *j*. Введем вектор *PE* размерности *h*+1, т. к. $PE_k$– вероятность события $E_k$, тогда: $PR = DP * PE$.

Матрица заполняется в соответствии с существующими данными об архитектуре системы.

***Матрица воздействий***

Компоненты архитектуры могут перестать правильно функционировать в результате нарушения безопасности, вызванного вредоносным воздействием. Для этого определимпотенциальный набор угроз.

Пусть $T_1, T_2 \ldots, T_p$ – реализовавшиеся угрозы, а $T_{p+1}$ – не реализовавшиеся угрозы. Вектор *PT* размерности *p+1* представляет собой:

- $PT_q$ — вероятность того, что угроза $T_q$ реализовалась в процессе работы ($1 \le q \le p$).
- $PT_{p+1}$ — вероятность того, что ни одна угроза не реализовалась в процессе работы.

Тогда получим:$PE_k = \sum_{q=1}^{p+1} P(E_k|T_q) * PT_q$.

Пусть *IM* — матрица воздействий размерности $h + 1 \times p + 1$, где строки *k* и столбцы *q* отражают вероятность того, что компонент $C_k$ отказал в связи с реализацией угрозы $T_q$ (или того, что угрозы не реализовались).

*PT* — вектор размерности $p + 1$, $PT_q$– вероятность того, что угроза $T_q$ реализовалась. Тогда $PE = IM * PT$.

Матрица заполняется в соответствии с возможными угрозами и оценками вероятности их появления. *PT* заполняется, исходя из возможного поведения нарушителей, особенностей системы, подверженности угрозам и т. д.

В результате, исходя из полученных матриц и вектора угроз, получим вектор *MFC*:

$MFC = ST * DP * IM * PT$.

## 3. Применение модели оценки рисков для систем облачной архитектуры

Рассмотрим возможность применения разработанной риск-модели для систем облачной архитектуры. Для этого необходимо определить существующие требования безопасности, заинтересованные стороны и их участие в этих требованиях и архитектурных компонентах системы.

***Матрица потерь***

Будем считать, что основными требованиями безопасности для систем, функционирующих на основе технологии облачных вычислений (ОВ) являются: доступность, полнота и конфиденциальность. Рассмотрим эти требо-

DOI: 10.7256/2073-8560.2013.6.9585



*Таблица 1. Матрица потерь: стоимость потерь в результате невыполнения требований безопасности (тыс. долларов/час)*

| Заинтересованные стороны | Требования безопасности | | | | | | |
|---|---|---|---|---|---|---|---|
| | ДКД | ДАД | ПКД | ПАД | КСД | КЧД | КПД |
| ПР | 500 | 90 | 800 | 150 | 1500 | 1200 | 120 |
| КК | 150 | 40 | 220 | 80 | 250 | 180 | 60 |
| ГК | 60 | 20 | 120 | 50 | 2500 | 30 | 12 |
| ИК | 0,05 | 0,015 | 0,30 | 0,20 | 0,30 | 0,10 | 0,01 |

вания с учетом различного уровня важности данных, для которых они применяются.

*Доступность*: возможность пользователя получить доступ к своей информации в момент, когда она ему будет необходима. Недоступность данных может быть более или менее затратной в зависимости от важности данных для пользователя. Мы будем разделять их на две категории: критические и архивные данные.

*Полнота*: показывает, что данные пользователя защищены от потерь или повреждения в результате вредоносного воздействия или непредусмотренных действий. Нарушение полноты может иметь различные последствия и быть более или менее затратным в зависимости от важности данных для пользователя.Выделим две категории: для критичных и для архивных данных.

*Конфиденциальность*: показывает, что данные пользователя защищены от несанкционированного доступа. Нарушение конфиденциальности может принести больше или меньше потерь пользователю в зависимости от уровня их конфиденциальности. Данные могут быть разделены на три категории: секретные, частные, публичные.

Для данной модели будем предполагать, что мы имеем дело с семью требованиями безопасности:

- ДКД: доступность к критическим данным.
- ДАД: доступность к архивным данным.
- ПКД: полнотакритических данных.
- ПАД: полнотаархивных данных.
- КСД: конфиденциальность секретных данных.
- КЧД: конфиденциальность частных данных.
- КПД: конфиденциальность публичных данных.

Будем считать, что провайдер услуг принимает в расчет важность данных и устанавливает приоритет выполнения более важных требований. Также будем считать, что все клиенты обладают равными правами и их данные защищаются одинаково, таким образом, если провайдер не может обеспечить выполнение определенных требований безопасности, то данная угроза распространяется для всех пользователей.

Для систем ОВ существует три класса заинтересованных сторон: провайдер услуг, корпорации или организации (юридические лица), индивидуальные пользователи (физические лица).

Пусть мы имеем дело с провайдером (ПР) и тремя клиентами: корпоративным клиентом (КК), государственным клиентом (ГК), индивидуальным клиентом (ИК).

В табл. 1 показаны потери заинтересованных сторон, рассчитанные в тыс. долларов на час операционного времени.

***Матрица зависимости***

Благодаря виртуализации системы ОВ оптимизируют затраты на ресурсы, позволяя пользователям использовать множество

DOI: 10.7256/2073-8560.2013.6.9585



*Таблица 2. Матрица зависимости*

| Требования безопасности | Компоненты | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Браузер | Прокси сервер | Роутер/ МЭ | Загрузочный балансировщик | Веб сервер | Сервер приложений | БД | Сервер резервного копирования | Сервер хранения | Нет сбоев |
| ДКД | 1 | 1 | 1 | 1 | 0,44 | 0,28 | 1 | 0,01 | 1 | 0 |
| ДАД | 1 | 1 | 1 | 1 | 0,44 | 0,28 | 0,28 | 0,01 | 1 | 0 |
| ПКД | 0,14 | 0,14 | 1 | 1 | 0,44 | 0,14 | 1 | 0,01 | 1 | 0 |
| ПАД | 0,14 | 0,14 | 1 | 1 | 0,44 | 0,14 | 0,14 | 0,01 | 1 | 0 |
| КСД | 0,44 | 0,14 | 1 | 1 | 0,44 | 0,44 | 0,44 | 0,01 | 0,44 | 0 |
| КЧД | 0,44 | 0,14 | 1 | 1 | 0,44 | 0,44 | 0,44 | 0,01 | 0,44 | 0 |
| КПД | 0,44 | 0,14 | 1 | 1 | 0,44 | 0,44 | 0,44 | 0,01 | 0,44 | 0 |

| Угрозы | |
|---|---|
| МВМ | Мониторинг виртуальной машины |
| КВМ | Коммуникации между ВМ и хостом |
| МодМВ | Модификация (изменение) ВМ |
| ВВМ | Размещение вредоносного образа ВМ в физической системе |
| МДВМ | Мониторинг ВМ другими ВМ |
| КМВМ | Коммуникации между ВМ |
| МобВМ | Мобильность ВМ |
| DoS | Отказ в обслуживании |
| FA | Flooding attacks (флуд атаки) |
| ПД | Потеря, кража данных |
| ВА | Внутренние агенты |
| КАУТ | Кража аккаунта, трафика, услуг |
| НПП | Нарушение правил пользования |
| НПИ | Небезопасный программный интерфейс |
| Нет | Нет угроз |

*Таблица 3. Матрица воздействий*

| Компоненты | Угрозы | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | МВМ | КВМ | МодМВ | ВВМ | МДВМ | КМВМ | МобВМ | DoS | FA | ПД | ВА | КАУТ | НПП | НПИ | нет |
| Браузер | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,02 | 0,01 | 0 | 0,03 | 0,02 | 0 | 0,03 | 0 |
| Прокси | 0,01 | 0,05 | 0 | 0,01 | 0,01 | 0,05 | 0,05 | 0,02 | 0,01 | 0 | 0,005 | 0,02 | 0,01 | 0 | 0 |
| Р/ФВ | 0,03 | 0,05 | 0,033 | 0,03 | 0,03 | 0,05 | 0,05 | 0,06 | 0,04 | 0 | 0,005 | 0,02 | 0,01 | 0,01 | 0 |
| Балансировщик | 0,02 | 0,003 | 0 | 0,01 | 0,02 | 0,003 | 0,003 | 0,06 | 0,04 | 0 | 0,005 | 0,02 | 0,01 | 0,01 | 0 |
| Веб сервер | 0,03 | 0,003 | 0,033 | 0 | 0,03 | 0,003 | 0,003 | 0,02 | 0,04 | 0 | 0,01 | 0,02 | 0,01 | 0,01 | 0 |
| Прил. сераер | 0,02 | 0,003 | 0,033 | 0,06 | 0,02 | 0,003 | 0,003 | 0,036 | 0,04 | 0 | 0,05 | 0,02 | 0,01 | 0,07 | 0 |
| БД | 0,001 | 0 | 0,033 | 0,04 | 0,001 | 0 | 0 | 0,036 | 0,04 | 0,05 | 0,03 | 0,02 | 0,01 | 0,06 | 0 |
| Бекап сервер | 0,001 | 0 | 0 | 0,04 | 0,001 | 0 | 0 | 0,036 | 0,04 | 0,05 | 0,03 | 0,02 | 0,01 | 0,06 | 0 |
| Хранилище | 0,04 | 0,05 | 0 | 0,04 | 0,04 | 0,05 | 0,05 | 0,036 | 0,04 | 0,05 | 0,03 | 0,02 | 0,01 | 0,06 | 0 |
| Нет сбоев | 0,06 | 0,04 | 0,03 | 0,03 | 0,06 | 0,04 | 0,04 | 0,01 | 0, 02 | 0,01 | 0,02 | 0,05 | 0,06 | 0,005 | 1 |

DOI: 10.7256/2073-8560.2013.6.9585



*Таблица 4. Вектор угроз*

| Угрозы | Вероятность |
|---|---|
| МВМ | $8{,}063*10^{-4}$ |
| КВМ | $8{,}063*10^{-4}$ |
| МодМВ | $8{,}063*10^{-4}$ |
| ВВМ | $8{,}063*10^{-4}$ |
| МДВМ | $40{,}31*10^{-4}$ |
| КМВМ | $40{,}31*10^{-4}$ |
| МобВМ | $40{,}31*10^{-4}$ |
| DoS | $14{,}39*10^{-4}$ |
| FA | $56{,}44*10^{-4}$ |
| **Угрозы** | **Вероятность** |
| ПД | $5{,}75*10^{-4}$ |
| ВА | $6{,}623*10^{-4}$ |
| КАУТ | $17{,}277*10^{-4}$ |
| НПП | $17{,}277*10^{-4}$ |
| НПИ | $29{,}026*10^{-4}$ |
| нет | 0,9682 |

*Таблица 5. Стоимость потерь для заинтересованных сторон*

| Заинтересованные стороны | Стоимость |
|---|---|
| ПР | 15,20443 |
| КК | 3,53839 |
| ГК | 8,98502 |
| ИК | 0,00341 |

приложений и функций на одном, а не на множестве устройств. Рассмотрим уровневую организацию ОВ:

- базовые составляющие: браузер, прокси-сервер, роутер, межсетевой экран (МЭ) и загрузочный балансировщик;
- облачные сервисы: веб сервер, сервер приложений, база данных, сервер хранения и восстановления информации;
- пользовательские инструменты.

Предположим, что за раз происходит сбой лишь одного компонента и, учитывая случай, когда все компоненты работают, построим матрицу.

***Матрица воздействий***

Следующий шаг — это построение матрицы воздействий. Системы ОВ подвержены множеству типов угроз, которые можно разделить на три категории:

1) Угрозы безопасности, идущие от хоста — этот класс угроз включает: угрозы связи между виртуальной машиной (ВМ) и хостом, мониторинг виртуальной машины, изменения виртуальной машины;

2) Размещение вредоносного образа ВМ на физической системе: включает угрозы безопасности, происходящие от атак на пользователей и датацентры, потери и утечку информации, вредоносное воздействие и т. д.

3) Небезопасный программный интерфейс: включает угрозы, происходящие от особенностей ВМ.

В данном примере будем учитывать четырнадцать угроз и случай, когда нет угрозы.

DOI: 10.7256/2073-8560.2013.6.9585



Нам необходимо знать вероятность возникновения каждой угрозы в час. Также необходимо указать значения вектора угроз, полученные в результате изучения системы.

Используя полученные матрицы и вектор угроз (таблица 4) можно посчитать стоимость потерь, вызванных ошибкой для каждой из сторон (таблица 5).

Потери для сторонявляются достаточно большими. Для того чтобы их сократить необходимо выявить уязвимости системы. Соотносим их с внешними и внутренними угрозами, ипринимаем необходимые контрмеры.

Подобное уточнение позволяет принять более обоснованные контрмеры. В данном случае — добавить межсетевой экран, прокси- и антивирусный сервер.

## Заключение

В данной работе была рассмотрена модель анализа рисков ИБ и возможность ее использования для случая ОВ. Хотя требуется дальнейшее уточнение составляющих частей модели, даже в таком виде возможно ее успешное применение. Приведен пример использования данной модели, дающей правомерные оценки рисков, и подтверждающий, что она может быть применена для принятия решений.

## Библиография

1. Zhang Jian Xun, Gu Zhi Min. Surey of research progress on cloud computing.Application Research of Computers, 2010, 27 (2).— PP. 429–433.
2. FENG Deng Guo, ZHANG Min, ZHANGYan, XUZhen.Study on Cloud Computing Security. Journal of Software, 2011, 22 (1).— PP. 71–83.
3. Michael Armbrust, Armando Fox, ReanGriffith.Above The Clouds: A Berkeley View of Cloud Computing. 2009, 2. EECS Department University of California, Berkeley Technical Report No. UCB /EECS 200928.http: //www.eecs. erkeley.edu /Pubs /TechRpts/2009/EECS-2009–28.pdf.
4. Царегородцев А. В., Качко А. К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2011.—№ 5.— С. 25–34.
5. Царегородцев А. В., Качко А. К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2012.—№ 1 (18).— С. 46–59.
6. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800–37, Revision 1,.
7. Steve Elky. An Introduction to Information System Risk Management-SANS Institute, 2007.

## References (transliterated)

1. Zhang Jian Xun, Gu Zhi Min. Surey of research progress on cloud computing.Application Research of Computers, 2010, 27 (2).— PP. 429–433.
2. FENG Deng Guo, ZHANG Min, ZHANGYan, XUZhen.Study on Cloud Computing Security. Journal of Software, 2011, 22 (1).— PP. 71–83.
3. Michael Armbrust, Armando Fox, ReanGriffith.Above The Clouds: A Berkeley View of Cloud

 

DOI: 10.7256/2073-8560.2013.6.9585



Computing. 2009, 2. EECS Department University of California, Berkeley Technical Report No. UCB /EECS 200928.http: //www.eecs. erkeley.edu /Pubs /TechRpts/2009/EECS-2009–28.pdf.
4. Tsaregorodtsev A. V., Kachko A. K. Obespechenie informatsionnoi bezopasnosti na oblachnoi arkhitekture organizatsii // Natsional'naya bezopasnost».— M.: Izd-vo «NB Media», 2011.— № 5.— S. 25–34.
5. Tsaregorodtsev A. V., Kachko A. K. Odin iz podkhodov k upravleniyu informatsionnoi bezopasnost'yu pri razrabotke informatsionnoi infrastruktury organizatsii // Natsional'naya bezopasnost».— M.: Izd-vo «NB Media», 2012.—№ 1 (18).— S. 46–59.
6. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800–37, Revision 1,.
7. Steve Elky. An Introduction to Information System Risk Management-SANS Institute, 2007.