УДК 006.72
doi:10.15217/issn1684-8853.2016.6.85

МЕТОД ВЫБОРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С УЧЕТОМ КРИТЕРИЯ КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЯ

Е. В. Попова[a]***,*** *старший преподаватель*
[a]*Смольный институт Российской академии образования, Санкт-Петербург, РФ*

Постановка проблемы: *при наличии нескольких вариантов системы защиты информации для данного предприятия необходимо выбрать многокритериальный оптимизационный вариант, который опирается на количественное значение конкурентоспособности предприятия. Методики такого выбора отсутствуют.* ***Цель исследования:*** *определение метода выбора наилучшего варианта системы защиты информации для повышения защищенности от угроз нарушения информационной безопасности предприятия.* ***Результаты:*** *описан модифицированный метод рандомизированных сводных показателей, позволяющий решить многокритериальную оптимизационную задачу. В качестве критерия выбора системы защиты информации предлагается количественное значение конкурентоспособности предприятия. Предложен метод прогнозирования снижения ущерба от нарушения информационной безопасности после внедрения системы защиты информации.* ***Практическая значимость:*** *предложенная модель повышения информационной безопасности с учетом критерия обеспечения конкурентоспособности предприятия позволяет повысить состояние защищенности от угроз нарушения информационной безопасности предприятия.*

Ключевые слова *— система защиты информации, конкурентоспособность предприятия, информационная безопасность.*

Введение

Проблемы информационной безопасности (ИБ) актуализируются на предприятиях с ростом информационных ресурсов, баз данных, с применением информационных технологий. При планировании деятельности по повышению защищенности от угроз нарушения ИБ перед предприятиями стоит выбор разработки или использования готовых средств защиты информации. Разработка и создание средств защиты информации требуют значительных финансовых вложений и получения лицензий Минобороны России, ФСБ России, Федеральной службы по техническому и экспертному контролю (ФСТЭК) России [1]. Готовые средства защиты представлены на рынке в разных ценовых категориях. При создании системы защиты информации (СЗИ) мы будем ориентироваться на предприятия, использующие готовые средства защиты, стоимость которых ограничена допустимыми затратами на данном предприятии.

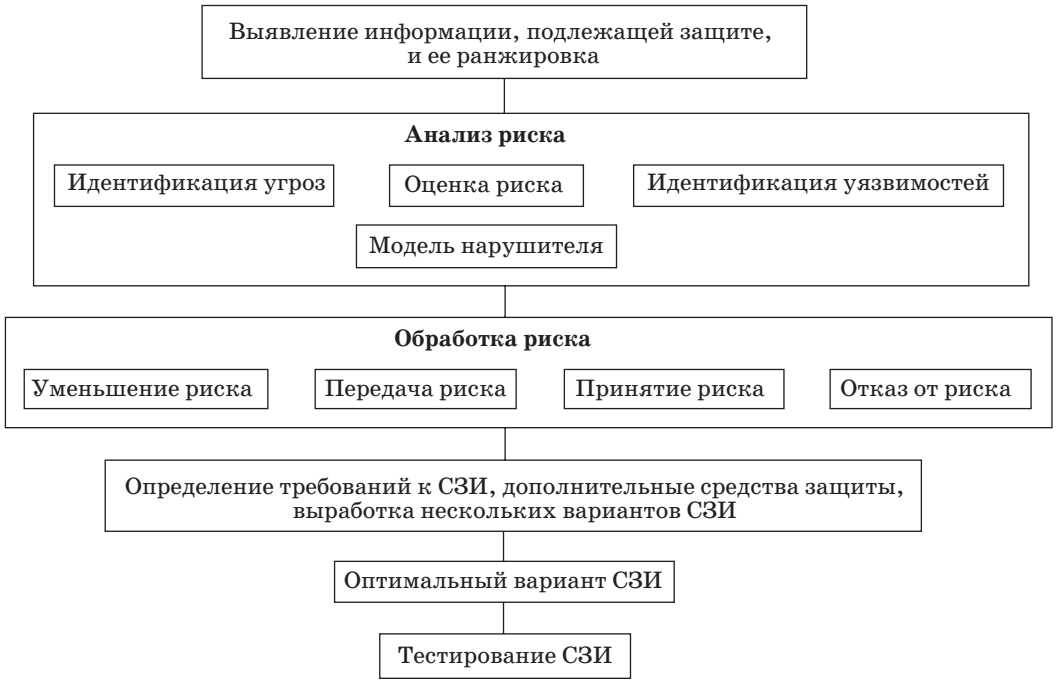
Основные задачи построения СЗИ

Согласно ГОСТ РФ 50922-2006: «система защиты информации: Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации» [2]. «При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется: <...> принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе...» [3].

Построение СЗИ — это комплексный поэтапный процесс, начинающийся с определения цели СЗИ. Целью является повышение ИБ, оцениваемой по критерию обеспечения конкурентоспособности предприятия.

В приказе ФСТЭК говорится, что «для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации» [3]. На предприятии формируется самостоятельное подразделение, которое занимается проблемами информационной безопасности — служба информационной безопасности (СИБ). Прописывается политика ИБ, согласованная с бизнес-процессами предприятия.

«Организационные и технические меры защиты информации реализуются в рамках системы защиты информации информационной системы в зависимости от информации, содержащейся в информационной системе» [3]. Сначала информация делится на общедоступную и ограниченного доступа. В информации ограниченного доступа выделяют информацию, составляющую государственную тайну и конфиденциальную. Если предприятие негосударственное, выбранную информацию можно ранжировать по стоимости информационного ресурса. Определив, что нужно защищать, переходят к анализу рисков.



■ ***Рис. 1.*** Схема построения СЗИ

Проводится идентификация угроз и уязвимостей имеющихся активов.

«Классификация угроз осуществляется по следующим признакам: по виду защищаемой информации; по видам возможных источников угроз безопасности; по типу информационной системы (ИС), на которую направлены угрозы; по способу реализации угроз безопасности; по виду несанкционированных действий; по используемой уязвимости; по объекту воздействия» [4]. Реализация угроз возможна при наличии уязвимостей. В список уязвимостей для предприятия включают: уязвимости программного обеспечения (ПО), уязвимости системного ПО, уязвимости прикладного ПО. Можно пользоваться единой базой данных Common Vulnerabilities and Exposures.

Затем строится модель нарушителя — описание потенциальных нарушителей правил разграничения доступа. Следующий этап — обработка риска, т. е. уменьшение риска, передача риска, принятие риска или отказ от риска.

Следующим этапом является формулирование требований к проектируемой системе. «Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком)» [3]. Выбирают дополнительные средства защиты, исходя из выявленных угроз, уязвимостей, задач предприятия и финансовых возможностей. Из нескольких вариантов СЗИ выбирается оптимальный по установленным критериям. Последним этапом проводится тестирование СЗИ. Этапы построения СЗИ представлены на рис. 1.

Служба ИБ проводит регистрацию событий и инцидент-менеджмент; контроль целостности, антивирусного ПО, политик, управления уязвимостями; анализ трафика. Необходимо выбирать наилучший вариант СЗИ для повышения состояния защищенности предприятия, используя критерий обеспечения конкурентоспособности предприятия.

Метод прогнозирования снижения ущерба от нарушения ИБ после внедрения СЗИ

Пусть $\mathbf{x}=(x_1, ..., x_m)$ — вектор исходных характеристик исследуемой системы. Обозначим условный эффект при изменении информационной безопасности $Э_{у\,ИБ}(\mathbf{x})$. Он равен разности ущербов до и после реализации СЗИ [5]:

$$Э_{у\,ИБ}(\mathbf{x}) = У_{до}(1-к_1(\mathbf{x})к_2(\mathbf{x})) = У_{до}(1-\rho(\mathbf{x})),$$
$$\rho(\mathbf{x}),\ к_1(\mathbf{x}),\ к_2(\mathbf{x}) \in [0;\ 1], \qquad (1)$$

где $У_{до}$ — величина ущерба от нарушений ИБ до внедрения СЗИ; $к_1(\mathbf{x})$, $к_2(\mathbf{x})$ — коэффициенты снижения количества нарушений и уменьшения тяжести нарушений соответственно до и после внедрения СЗИ; $\rho(\mathbf{x})$ — коэффициент изменения конкурентоспособности. При величине ущерба в денежном выражении $У_{пос}$ после внедрения СЗИ формулы (1) позволяют получить теоретические и реальные значения коэффициента изменения конкурентоспособности и условного эффекта (таблица).

Получив теоретическое значение коэффициента изменения конкурентоспособности, можно спрогнозировать снижение ущерба после внедре-

Теоретические значения	Реальные значения
$\rho(\mathbf{x})$ получен с помощью модифицированного метода рандомизированных сводных показателей (ММРСП)	$\rho(\mathbf{x}) = к_1(\mathbf{x})к_2(\mathbf{x})$
$Э_{у\ ИБ}(\mathbf{x}) = У_{до}(1 - \rho(\mathbf{x}))$	$Э_{у\ ИБ}(\mathbf{x}) = У_{до} - У_{пос}$

ния оптимального варианта СЗИ. В целях увеличения условного эффекта нужно выбрать минимальное значение коэффициента изменения конкурентоспособности при обеспечении ИБ (коэффициента относительного уменьшения ущерба). Для этого необходимо решить следующую оптимизационную задачу:

$$\rho(\mathbf{x}^0) = \min(\rho(\mathbf{x})),\ \rho \in [0; 1],$$
$$\mathbf{x}^0 \in X^d \text{ при ограничении } Z(\rho) \le Z^d, \qquad (2)$$

где $\mathbf{x}^0$ — оптимальное значение вектора; X^d — множество допустимых значений векторов числовых характеристик; Z^d — допустимые затраты для предприятия. Средства защиты информации выбираются из ценовой категории, которая позволяет ограничиться допустимыми затратами.

Необходимо выбрать наилучший вариант СЗИ, приводящий к повышению состояния защищенности от угроз нарушения информационной безопасности, характеристики которого обеспечивают минимум коэффициента изменения конкурентоспособности, учитывая допустимые затраты. Для решения этой задачи мы применим ММРСП.

При решении задач с несколькими критериями оптимальности ММРСП позволяет построить сводную оценку, которая объединяет значимость характеристик, и упорядочить объекты по предпочтительности [6, 7].

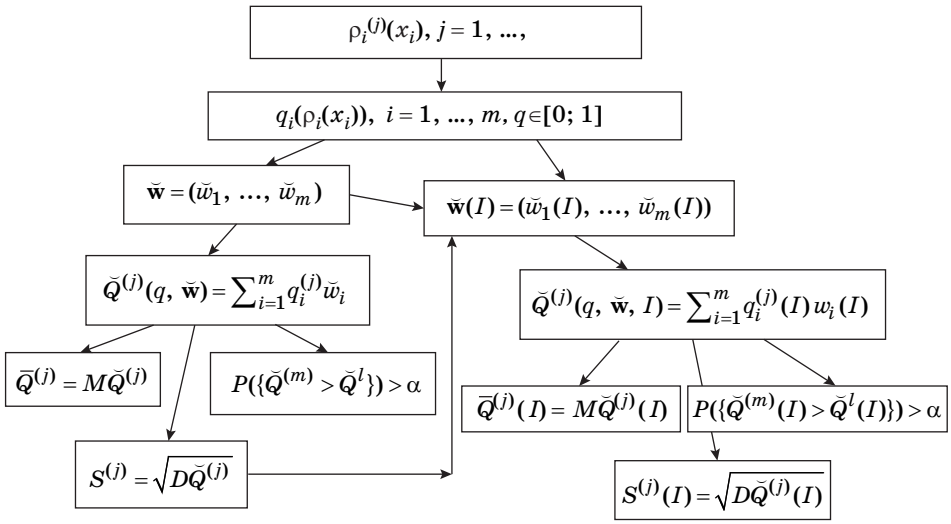
Модифицированный метод рандомизированных сводных показателей основан на экспертных оценках коэффициента изменения конкурентоспособности $\rho(\mathbf{x})$ по шкале каждого из критериев [5]. Мы оцениваем k вариантов СЗИ по m критериям. После нормировки $q_i(\rho_i(x_i))$ исходной матрицы рандомизированный вектор весовых коэффициентов $\breve{\mathbf{w}}$ формирует сводный показатель и его стохастические оценки. На рис. 2 представлена схема ММРСП.

Дополнительная неполная, неточная и нечисловая информация I повышает точность вычислений. По многокритериальному сводному показателю мы получаем оптимизационный многокритериальный вариант СЗИ для данного предприятия и обеспечение ИБ предприятия. Экспертные оценки формируются специалистами, которые соответствуют определенным требованиям.

«Эксперт (от лат. expertus — опытный, знающий, сведущий) — специалист, дающий заключение при рассмотрении какого-нибудь вопроса» [8]. Эксперты должны быть компетентными, опытными, эрудированными в смежных областях, объективными, иметь ученую степень. Эксперты должны пройти инструктаж, определить степень согласованности действий. Эксперты получают шкалу измерений, объект измерений, узнают, какое значение показателей является наилучшим. Коэффициент ранговой согласованности Кендалла — Смита определяется формулой

$$W = \frac{12S}{n^2(m^3 - m)}, \qquad (3)$$

где S — сумма квадратов отклонений суммы рангов каждого объекта экспертизы от среднего арифметического рангов; n — число экспертов; m — число оцениваемых объектов. W стремится к 0 при несогласованности и к 1 при обратной



■ ***Рис. 2.*** Общая схема ММРСП

ситуации. Выводы экспертов должны быть инвариантны относительно допустимых преобразований шкал измерений.

Используется метод индивидуальной оценки. Объект оценки получает определенное значение по оценочной шкале, а затем эти индивидуальные значения разных экспертов усредняются по Колмогорову [9].

Модель повышения ИБ по критерию обеспечения конкурентоспособности предприятия и расчет эффективности СЗИ

В работе [10] была выведена формула количественного подсчета конкурентоспособности предприятия при обеспечении информационной безопасности:

$$к_{пред} = \sum_{i=1}^{n} a_i b_i \frac{\alpha_i F_i + Э^i_{у\,ИБ}}{\alpha_i^б F_i^б} \frac{C_i^б + E_i^б}{C_i + E_i + Z_i}, \quad (4)$$

где a_i — доля товара в объеме продаж за анализируемый период, доли единицы; $\sum_{i=1}^{n} a_i = 1$; b_i — относительный вес рынка, на котором представлен товар предприятия; $\alpha_i F_i$ — коммерческая оценка качества; C_i — покупная цена продукции; E_i — сопутствующие затраты на использование; индекс «б» означает те же показатели, но по отношению к базовым товарам и услугам.

Модель повышения ИБ по критерию обеспечения конкурентоспособности предприятия отражают следующие соотношения: оптимизационная задача (2) и формула подсчета конкурентоспособности (4). Схема реализации модели представлена на рис. 3.

■ ***Рис. 3.*** Схема реализации модели повышения ИБ предприятия

В соответствии с приказом ФСТЭК России от 18 февраля 2013 г. № 21, «оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится организацией самостоятельно или с привлечением юридических лиц, имеющих соответствующую лицензию» [11]. При этом форма оценки эффективности, а также содержание и форма итоговых документов в данном приказе не установлены. В ГОСТ [2] под эффективностью СЗИ понимается степень соответствия результатов защиты информации поставленной цели. Целью является повышение ИБ, оцениваемой по критерию обеспечения конкурентоспособности предприятия. Выбирая наилучший вариант СЗИ по оптимальному значению коэффициента изменения конкурентоспособности, мы повышаем состояние защищенности предприятия от угроз нарушения ИБ с учетом критерия обеспечения конкурентоспособности предприятия. Следовательно, выбранный оптимизационный вариант СЗИ является эффективным.

Подсчет экономической эффективности важен для предпроектных расчетов и обоснования выделяемых затрат [12]. В этом случае эффективность СЗИ зависит от результатов и затрат, сбалансированных в приемлемой пропорции. При этом затраты не должны превышать Z^d [13]. Основным результатом при создании СЗИ является уменьшение ущерба в денежном выражении при реализации угроз ИБ. Поэтому за результаты реализации конкретной СЗИ следует принять максимальное значение $Э_{у\,ИБ}$ условного эффекта при усилении ИБ. Тогда экономическая эффективность СЗИ

$$E_{СЗИ} = \frac{У_{до}(1 - \rho(\mathbf{x}))}{Z} - 1, \quad (5)$$

где Z — затраты на создание СЗИ. Если итоговая разность больше нуля, то данная реализация СЗИ считается эффективной относительно отдачи от вложенных средств.

Заключение

Современные тенденции к увеличению общего количества кибер-атак, числа компаний, подвергающихся нападениям, и величины ущерба заставляют больше внимания уделять ИБ. Сопровождающие инциденты простои в работе, снижение производительности, потеря имиджа, репутационные проблемы приводят к убыткам не только в текущем периоде, но и влияют на деятельность предприятия в будущем. Выбор наилучшего варианта СЗИ с учетом критерия конкурентоспособности предприятия позволяет повысить состояние защищенности предприятия от угроз нарушения ИБ.

Литература

1. Официальный сайт Федеральной службы по техническому и экспертному контролю. http: www.fstec.ru (дата обращения: 18.02.2016).
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения: 18.04.2016).
3. Федеральная служба по техническому и экспертному контролю. Приказ от 11 февраля 2013 г. № 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 18.06.2016).
4. Федеральная служба по техническому и экспертному контролю. 15 февраля 2008 г. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. http://fstec.ru/component/attachments/download/289 (дата обращения: 18.06.2016).
5. **Попова Е. В.** Выбор варианта системы защиты информации по критерию обеспечения конкурентоспособности предприятия // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2(90). С. 155–160.
6. **Хованов Н. В., Федотов Ю. В.** Модели учета неопределенности при построении систем// Научные доклады НИИ менеджмента СПбГУ. 2006. № 28. С. 1–37.
7. **Hovanov N., Yudaeva M., Hovanov K.** Multicriteria Estimation of Probabilities on Basis of Expert Non-numeric, Non-exact and Non-complete knowledge// Abstracts of 18th Intern. Conf. on Multiple Criteria Decision Making, Chania (Greece), June 19–23, 2006. P. 102.
8. Общий толковый словарь русского языка. http://tolkslovar.ru/ie672.html (дата обращения: 18.07.2016).
9. **Колмогоров А. Н.** Математика и механика // Избранные труды / отв. ред. С. М. Никольский, сост. В. М. Тихомиров. — М.: Наука, 1985. Т. 1. С. 136–138.
10. **Попова Е. В.** Расчет конкурентоспособности малых предприятий сферы сервиса при усилении информационной безопасности // Вестник Российской академии естественных наук. 2012. № 16(3). С. 48–51.
11. Федеральная служба по техническому и экспертному контролю. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (дата обращения: 18.02.2016). www.fstec.ru.
12. **Маслова Н. А.** Методы оценки эффективности систем защиты информационных систем // Штучний інтелект. 2008. № 4. С. 253–264.
13. **Попова Е. В.** Эффективность системы защиты информации, выбранной по критерию обеспечения информации// Приборостроение. 2014. № 9. С. 19–22.

UDC 006.72
doi:10.15217/issn1684-8853.2016.6.85

Choosing an Information Protection System Taking into Account the Company Competitiveness

Popova E. V.[a], Senior Lecturer, serana5@inbox.ru
[a]Smol'nyi Institut RAO, 59, Poliustrovskii Pr., 195197, Saint-Petersburg, Russian Federation

Introduction: When an information protection system for a given company can be implemented in several ways, you have to choose a multi-criteria optimization variant based on a quantitative value of the company competitiveness. Techniques for such choice are not available. **Purpose:** The aim of this work is to find a method for choosing the best way of implementing an information protection system in order to improve the information security. **Results:** A modified method of randomized aggregates is proposed, which allows you to solve a multi-criteria optimization problem. As a criterion for choosing an information protection system, a quantitative value of the company competitiveness is offered. A method is proposed for predicting how the information security violation impact can be reduced after the information protection system is introduced. **Practical relevance:** The proposed model of improving the information security taking into account the company competitiveness criterion allows you to more efficiently protect a company from threats to its information security.

Keywords — Information Protection System, Company Competitiveness, Information Security.

References

1. *Ofitsial'nyi sait Federal'noi sluzhby po tekhnicheskomu i ekspertnomu kontroliu* [The Official Site of the Federal Service for Technical and Export Control]. Available at: www.fstec.ru (accessed 18 February 2016).
2. State Standard 0922-2006. Data Protection. Basic Terms and Definitions. Available at: http://docs.cntd.ru/document/gost-r-50922-2006 (accessed 18 April 2016).
3. *Federal'naia sluzhba po tekhnicheskomu i ekspertnomu kontroliu. Prikaz ot 11 fevralia 2013 g. N 17 ob utverzhdenii trebovanii o zashchite informatsii, ne sostavliaiushchei gosudarstvennuiu tainu, soderzhashcheisia v gosudarstvennykh informatsionnykh sistemakh* [The Federal Service for Technical and Expert Control. Order of February 11, 2013 N 17 on the Approval of the Data Protection Requirements, not the State Secret Contained in the State Information Systems] Available at: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed 18 June 2016).
4. *Federal'naia sluzhba po tekhnicheskomu i ekspertnomu kontroliu. Bazovaia model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: vypiska 15 fevralia 2008 g.* [The Federal Service for Technical and Expert Control. The Basic Model of Personal Data Security Threats at their Processing within the Information Systems of Personal Data: Out February 15, 2008] Available at: http://fstec.ru/component/attachments/download/289 (accessed 18 June 2016).
5. Popova E. V. Selecting Information Protection System by the Criterion of Ensuring the Competitiveness of Enterprises. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2014, no. 2(90), pp. 155–160 (In Russian).

6. Hovanov N. V., Fedotov Ju. V. The Models Account for the Uncertainty in the Construction of Systems. *Nauchnye doklady NII menedzhmenta* [Scientific Reports of Research Institute of Management]. SPbGU, 2006, no. 28, pp. 1–37 (In Russian).
7. Hovanov N., Yudaeva M., Hovanov K. Multicriteria Estimation of Probabilities on Basis of Expert Non-numeric, Non-exact and Non-complete Knowledge. *Abstracts of 18th Intern. Conf. on Multiple Criteria Decision Making*, Chania (Greece), June 19–23, 2006, p. 102.
8. *Ozhegov Tolkovyj Slovar'* [Official Web Site of General Dictionary of Russian Language]. Available at: http://tolkslovar.ru/ie672.html (accessed 18 July 2016).
9. Kolmogorov A. N. Mathematics and Mechanics. *Izbrannye trudy*, otv. red. S. M. Nikol'skij, sost. V. M. Tihomirov, Moscow, Nauka Publ., 1985, vol. 1, pp. 136–138 (In Russian).
10. Popova E. V. Calculation of the Competitiveness of Small Enterprises of Sphere of Service at Strengthening Information Security. *Vestnik Rossiiskoi akademii estestvennykh nauk*, 2012, no. 16(3), pp. 48–51 (In Russian).
11. *Prikaz FSTJeK Rossii ot 18 Fevralja 2013 g. № 21.* [Oficial'nyj Sajt Federal'noj Sluzhby po Tehnicheskomu i Jekspertnomu Kontrolju]. Available at: http: www.fstec.ru (accessed 18 February 2016).
12. Maslova N.A. Methods for Evaluating the Effectiveness of the Protection of Information Systems Systems. *Shtuchnii intelekt*, 2008, no. 4, pp. 253–264 (In Russian).
13. Popova E. V. The Effectiveness of the Protection of Information Systems, Selected by the Criterion of Providing Information. *Priborostroenie*, 2014, no. 9, pp. 19–22 (In Russian).