Оптимизация мероприятий аудита системы менеджмента информационной безопасности

Optimization of audit measures of the information security management system

Ключевые слова: информационная безопасность – information security; аудит систем менеджмента информационной безопасности – ISMS audit, audit planning; оптимальное планирование мероприятий аудита – optimum scheduling of audit measures.

Эффективность аудита систем менеджмента информационной безопасности определяется отношением достигнутых показателей качества к затраченным ресурсам. Разработка методов и методик, позволяющих повысить эффективность аудита, является актуальной задачей. Предложенная авторами методика на основе модели динамики показателя качества системы позволяет оптимально распределять временные (материальные) ресурсы по этапам аудита. Достоинство методики заключается в снижении временных (стоимостных) затрат аудита на 10–15% или в повышении качества оценивания.

The effectiveness of the ISMS audit is determined by the ratio of the achieved quality to used resources. The development of methods and techniques that improve the effectiveness of the audit is a vital task. Authors propose methods based on the model of factors dynamics of the quality system that optimally allocate time (material) resources on the audit stages. The advantage of this method is to reduce the time (cost) audit spends by 10-15% or to improve the estimation quality.

ШАГО / SHAGO F.
Федор Николаевич
(dreamcast73@yandex.ru)
ФГБОУ ВПО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (НИУ ИТМО), аспирант.
г. Санкт-Петербург

ЗИКРАТОВ / ZIKRATOV I.
Игорь Алексеевич
(zikratov@cit.ifmo.ru)
доктор технических наук, профессор.
НИУ ИТМО, заведующий кафедрой Безопасных информационных технологий.
г. Санкт-Петербург

ВВЕДЕНИЕ

Система менеджмента информационной безопасности (СМИБ) (information security management system, ISMS) – часть общей системы менеджмента организации, основанная на подходе бизнес-рисков, по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности (ИБ) [1]. Аудит является ключевым звеном в системе разработки, построения и использования СМИБ. По результатам проведенного аудита заказчик принимает решение о соответствии построенной или существующей СМИБ организации требованиям законодательных актов и стандартов Российской Федерации (РФ).

Планирование мероприятий аудита является важной и определяющей частью проверки СМИБ. При аудите СМИБ привлекается персонал организации, осуществляется доступ к документам и базе данных организации, изучается существующая автоматизированная информационная система (ИС) организации [2, 3], что существенно влияет на объем материальных и временных затрат на проведение аудита. Правильное распределение ресурса при планировании мероприятий аудита в значительной степени определяет эффективность расходования временных, материальных и трудовых резервов аудита.

В большинстве случаев в процессе планирования ресурс аудита распределяется на основе имеющегося опыта, директивных указаниях руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) и государственных стандартов РФ с применением общеизвестных методов (например, по диаграмме Ганта, Program PERT (Project Evaluation and Review Technique – техника оценки и анализа программ (проектов)) [2, 3]. Оптимизация распределения ресурса может проводиться в начале проверок. Выполнение программы аудита производится в

соответствии с составленным планом, и дальнейших корректировок плана не производится [3]. Очевидно, что эффективность аудита будет определяться отношением достигнутых показателей качества к затраченным ресурсам. Таким образом, возникает важная и актуальная задача разработки методов и методик оптимизации планирования аудита СМИБ, позволяющая повысить эффективность аудита.

Предлагаемая методика оптимизации планирования мероприятий аудита СМИБ позволяет осуществлять корректировку программы аудита, учитывая полученные результаты на этапах аудита СМИБ.

ОБОСНОВАНИЕ МЕТОДИКИ ОПТИМИЗАЦИИ ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ АУДИТА

Постановка задачи оптимизации проведения аудита СМИБ может быть в следующих вариантах:

$$\begin{cases} C(U,t) \to \min; \\ U(C,t) > U_{\text{Т}}; \\ t < t_{\text{доп}}, \end{cases}$$

или

$$\begin{cases} U(C,t) \to \max; \\ C(U,t) < C_{\text{доп}}; \\ t < t_{\text{доп}}, \end{cases}$$

где C ($C_{\text{доп}}$) – затраты (допустимые затраты) на проведение аудита СМИБ; U ($U_{\text{Т}}$) – уровень защищенности информации (эффективности СМИБ) в проверяемой организации (требуемый уровень эффективности СМИБ); $t < t_{\text{доп}}$ – длительность проведения аудита (допустимая длительность).

Основная трудность решения задачи в данной постановке заключается в установлении зависимости стоимости проведения аудита СМИБ организации от свойств ИС и условий проведения аудита [2, 4]. Иная постановка задачи связана с выбором в качестве показателя эффективности СМИБ отношения

$$\overline{U_C} = \frac{U - U_0}{C} = \frac{\Delta U}{C},$$

где U_0, U – эффективность СМИБ до и после проведения аудита.

Показатель U_C целесообразно использовать, если задана одна из величин ΔU или C. В противном случае изменение числителя может компенсироваться соответствующим изменением знаменателя, что приводит к ошибочному решению.

При установлении области допустимых значений $(U/C)_{\text{доп}}$, предпочтение отдается системе, обеспечивающей относительно большую вероятность

$$P = p\left(\frac{\Delta U}{C} \in \left\{\frac{\Delta U}{C}\right\}_{\text{доп}}\right).$$

Необходимой и составной частью решения задач проведения аудита СМИБ является построение модели динамики показателя качества ИБ в процессе аудита. Модель необходима для составления плана проведения аудита. Пусть качество СМИБ характеризуется уровнем рисков [5–7]

$$R = \sum_i V_i \cdot p_i(V_i),$$

связанных с вероятностями реализации угроз безопасности в отношении ресурсов ИС, где V_i – ущерб, ожидаемый при реализации угрозы и $p_i(V_i)$ – вероятность риска ИБ (например, потеря конфиденциальности, целостности и доступности данных организации). Выразим p_i через вероятность предотвращения риска p_{ai}:

$$p_i(V_i) = (1\text{-}p_{ai}(V_i)),$$

тогда

$$R = \sum_i V_i \cdot (1 - p_{ai}(V_i)).$$

Пусть p_{ai} – предельно достижимый на рассматриваемом этапе аудита показатель качества ИБ. Тогда приращение показателя в результате внедрения доработок и уточнения политик безопасности СМИБ после проведения этапа аудита можно представить в виде

$$dp_i = \theta_i \left(p_{ani} - p_{ai}\right) dt,$$

где θ_i – средняя интенсивность изменений, вносимых в СМИБ после очередного этапа аудита.

В качестве модели динамики показателя качества СМИБ используем математическую модель динамики показателя качества при известной зависимости доработок политик безопасности от временных затрат на проведение аудита:

$$p_{ai} = p_{ani} - \left(p_{ani} - p_{0ai}\right)e^{-\theta_i(t_i - t_{0i})} = \\ = p_{ani} - \left(p_{ani} - p_{0ai}\right)e^{-\theta_i\tau_i}. \quad (1)$$

По аналогии можно получить выражение для стоимости, заменив продолжительность аудита затратами на проведение.

Поскольку вместо p_{ai} вероятности предотвращения риска ИБ могут использоваться другие показатели качества, зависимость (1) можно представить в виде:

$$U_i = a_i - \left(a_i - U_{0i}\right)\cdot e^{-\theta_i\tau_i}; \quad (2)$$

$$U_i = b_i - \left(b_i - U_{0i}\right)\cdot e^{-\gamma_i\tau_i}, \quad (3)$$

где a_i, b_i имеют смысл предельно достижимых на i-ом этапе аудита показателей качества проверяемой СМИБ; γ_i – средняя интенсивность изменений, вносимых в СМИБ, подсчитываемых относительно выделенных затрат С.

При правильно организованном аудите уровень и количество рисков ИБ по мере доработки политик безопасности уменьшается и соответственно справедливы соотношения $a_i > a_{i-1}$, $b_i > b_{i-1}$, $\gamma_i < \gamma_{i-1}, \theta_i < \theta_{i-1}$.

Исходя из вышесказанного, задачу составления плана мероприятий аудита СМИБ можно сформулировать как поиск оптимального распределения времени (средств) по этапам аудита.

Для получения критерия, используя уравнения динамики показателя качества (2) и (3), можно рассчитать общее время (стоимость) аудита, суммируя длительности каждого i-го этапа аудита:

$$T = \sum_{i=1}^{k}\tau_i = \sum_{i=1}^{k}\frac{1}{\theta_i}\ln\frac{a_i - U_{0i}}{a_i - U_i};$$

$$C = \sum_{i=1}^{m}\frac{1}{\gamma_i}\ln\frac{b_i - U_{0i}}{b_i - U_i},$$

где k, m – количество этапов аудита.

Из формул видно, что продолжительность аудита (стоимость проведения аудита) будет определяться положением точек перехода от одного этапа к другому, т.е. значениями U_i, $i = 1, k-1$ ($U_k > U_\text{T}$, U_T – требуемое значение). Тогда задача сводится к нахождению значений U_i, обеспечивающих минимальное время проведения аудита (или минимум стоимости аудита) при условии, что после k этапов обеспечивается достижение требуемого уровня U_T. В соответствии с постановкой задачи решение, с помощью метода динамического программирования, ищется в условиях многошагового расчета, причем состояние системы на i-м шаге зависит только от состояния системы на (i–1)-м шаге.

Исходя из принципа динамического программирования, оптимизацию проводят от конечного k-го этапа. В качестве критерия используем продолжительность аудита. Для произвольного шага

$$\Phi_i = \tau_k + \tau_{k-1} + \ldots + \tau_i.$$

На первом этапе $\Phi_k = \tau_k$ и справедливо $\min\Phi_k = \min\tau_k$.

На следующем этапе

$$\Phi_{k-1} = \tau_k + \tau_{k-1} = \frac{1}{\theta_k}\ln\frac{a_k - U_{0k}}{a_k - U_k} + \\ + \frac{1}{\theta_{k-1}}\ln\frac{a_{k-1} - U_{0k-1}}{a_{k-1} - U_{k-1}}.$$

С учетом того, что $U_k = U_\text{T}$, а U_k–1 = U_{0k}, зависимость Φ_{k-1} можно представить в виде

$$\Phi_{k-1} = \frac{1}{\theta_k}\ln\frac{a_k - U_{0k}}{a_k - U_\text{T}} + \frac{1}{\theta_{k-1}}\ln\frac{a_{k-1} - U_{0k-1}}{a_{k-1} - U_{0k}}.$$

Если не использовать модель, то решение сводится к выводу $\Phi_1 = 0$, $U_0 = U_k = U_\text{T}$.

Условие оптимального перехода от k-го этапа к (k–1) этапу можно получить, продифференцировав слагаемые Φ_{k-1}, и после вычислений, приравняв результаты, получим

$$\theta_k\left(a_k - U_{0k}\right) = \theta_{k-1}\left(a_{k-1} - U_{0k}\right).$$

Левая часть уравнения характеризует скорость роста U на k-ом этапе $\left.\frac{dU_k}{d\tau_k}\right|_{\tau_k}$, а правая – скорость роста на (k–1) этапе $\left.\frac{dU_{k-1}}{d\tau_{k-1}}\right|_{\tau_{k-1}}$.

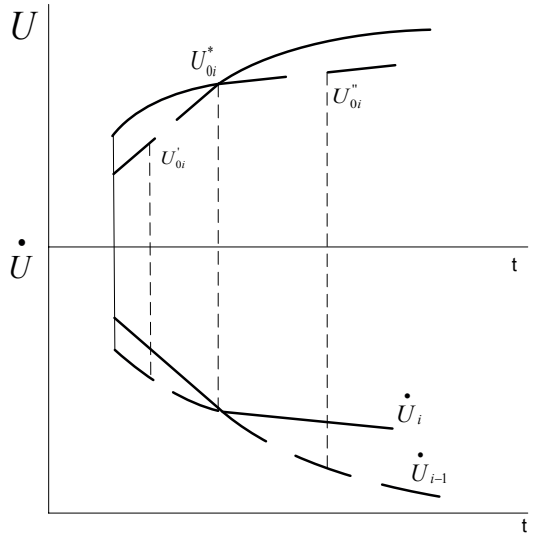

Рис. 1. Точка U^*_{0i} оптимального перехода от *k*-го этапа аудита к (*k*–1) этапу. На совмещенных графиках, отражающих уровень показателя качества U и скорость его прироста $\dot{U}$ в зависимости от времени, сплошной линией обозначена оптимальная траектория, пунктиром обозначены траектории изменения показателя качества U'_{0i} на первом этапе и U''_{0i} соответственно на втором, без оптимизации.

Следовательно, оптимальному моменту перехода от *k*-го этапа к ($k-1$) этапу аудита соответствует точка равенства скоростей изменения U на ($k-1$) и k-ом этапах (рис. 1).

При дальнейшем решении задачи получаем условие оптимального перехода от произвольного (i–1) уровня к i-му уровню:

$$\theta_i\left(a_i - U^*_{0i}\right) = \theta_{i-1}\left(a_{i-1} - U^*_{0i}\right),$$

откуда

$$U^*_{0i} = \frac{\theta_i a_i - \theta_{i-1} a_{i-1}}{\theta_i - \theta_{i-1}}. \qquad (4)$$

Зависимость (4) позволяет определить условия, при которых обеспечивается минимальное время прохождения отрезка траектории $U_\text{Т} - U_0$ (максимальная скорость движения). Из графика на рис. 1 видно, что если движение (переход к новому этапу аудита) начинается при $U_{0i} < U^*_{0i}$, то происходит потеря времени. По той же причине невыгодно начинать движение по i-ой кривой при $U_{0i} < U^*_{0i}$. Оптимальная продолжительность аудита:

$$T^* = \sum_{i=1}^{k} \tau_i = \sum_{i=1}^{k} \frac{1}{\theta_i} \ln \frac{a_i - U^*_{0i-1}}{a_i - U^*_{0i}}.$$

Аналогично задача решается для критерия стоимости:

$$C^* = \sum_{i=1}^{m} C_i = \sum_{i=1}^{m} \frac{1}{\gamma_i} \ln \frac{b_i - U^*_{0i-1}}{b_i - U^*_{0i}}.$$

Таким образом, методика включает в себя следующие процедуры, выполняемые в процессе оптимизации распределения ресурса аудита при планировании аудита СМИБ.

1. С помощью формул (2), (3) произвести расчет планируемого роста показателя эффективности СМИБ U_i на этапах аудита.

2. Используя выражение (4), рассчитать точки оптимального перехода U^*_{0i} между мероприятиями для исходного расчета плана.

3. Выполнить мероприятие аудита и оценить достигнутый уровень эффективности a_i проверяемой СМИБ на i-ом этапе аудита.

4. Произвести перерасчет точек оптимального перехода U^*_{0i} между мероприятиями аудита, исходя из полученной в п. 3 оценки.

5. Проверить условие перехода на следующий этап аудита $a_i \geq U^*_{0i}$, если условие выполняется, произвести перераспределение неизрасходованного ресурса i-го этапа на следующие этапы аудита.

6. Выполнять пп. 3–5 до получения требуемого уровня $U_\text{Т}$ СМИБ.

Таким образом, основные пути сокращения времени (затрат) на аудит СМИБ:

– уменьшение $\tau_i(C_i)$ за счет повышения качества планирования, уточнения моделей динамики показателя качества ИБ после проведения очередного мероприятия аудита;

– повышение эффективности изменений в СМИБ по улучшению ИБ.

ПРИМЕРЫ ПРИМЕНЕНИЯ МЕТОДИКИ ОПТИМИЗАЦИИ ПЛАНИРОВАНИЯ МЕРОПРИЯТИЙ АУДИТА СМИБ

В ходе проведения аудита СМИБ в конкретной организации невозможно произвести оценку всех рисков ИБ [8, 9, 10], которым должна противостоять современная СМИБ. Отказы и недостатки самой СМИБ могут также оказать существенное влияние на программу проведения аудита. Использование апостериорных данных для очередного мероприятия аудита и коррекция модели показателя качества ИБ позволяет максимально приблизиться к оптимуму распределения ресурсов, выделенных на проведение аудита.

Например, узловым моментом планирования мероприятий аудита является распределение времени и материальных затрат между предварительным сбором данных и анализом документов и проведением аудита на месте (рис. 2).

Рассмотрим пример по определению оптимального времени между двумя этапами проведения аудита. Допустим, что динамика показателя качества СМИБ на каждом этапе аудита подчиняется экспоненциальному закону с известными параметрами [11]. С учетом этого сплошная и пунктирная кривые 1 будут соответствовать росту показателя качества СМИБ на этапе сбора данных и анализа документов по ИБ, а сплошная и пунктирная кривые 2 – на этапе аудита на месте.

Если весь выделенный ресурс использовать только на этапе аудита на месте и проводить его до достижения уровня показателя качества ИБ равному a_2, то для этого потребуется время t_{max}. На этапе работы с документами и сбора данных скорость роста показателя качества выше, чем на этапе аудита на месте, но предельно достижимый уровень показателя качества a_1 меньше заданного уровня $a_{эф}$, определенного требованиями к показателю качества СМИБ. Применив методику, можно рассчитать точку оптимального перехода A от одного этапа к другому, добившись максимальной скорости прироста показателя качества в процессе аудита. Тем самым, для сокращения общего времени (стоимости, количества итераций) аудита необходимо проводить этап сбора данных и

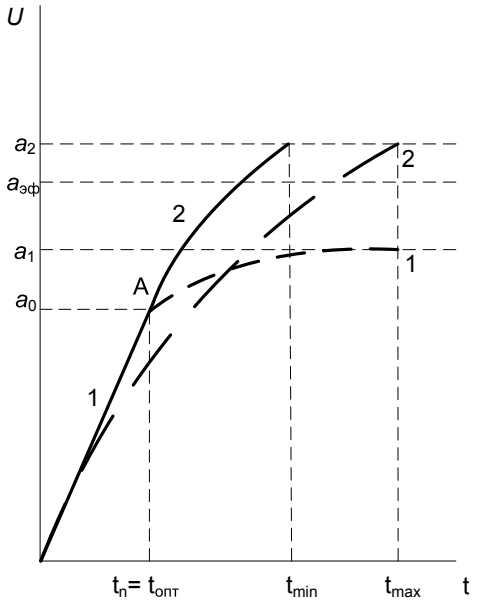

Рис. 2. Точка перехода (*A*) от сбора, обработки и анализа документов (сплошная и пунктирная кривые 1) к аудиту на месте (сплошная и пунктирная кривые 2), где a_0 – уровень показателя качества при достижении которого необходимо перейти к этапу аудита на месте; a_1 – предельно достижимый уровень показателя качества для этапа сбора, обработки и анализа документов; $a_{эф}$ – пороговое значение показателя качества определенное требованием к СМИБ; a_2 – достигнутый уровень показателя качества на этапе аудита на месте; $t_п$ – время перехода от этапа сбора, обработки и анализа документов к этапу аудита на месте, которое и является оптимальным временем $t_{опт}$

анализа документов до достижения оптимального уровня показателя качества a_0, соответствующего точке *A*. Окончательное достижение требуемого значения показателя качества U_T осуществлять на этапе местного аудита.

Пример второй. На этапе аудита на месте осуществлялись мероприятия по проверке политик безопасности в области предотвращения несанкционированного доступа к базе данных организации через локальную вычислительную сеть (ЛВС) организации.

Проводился анализ:

– механизмов безопасности на организационном уровне, политики безопасности организации по обеспечению режима ИБ;

– критических элементов сетевой инфраструктуры организации (межсетевых экранов, серверов, осуществляющих управление межсетевым взаимодействием, почтовых и DNS-серверов и т.д.);

– доступности внешних сетевых адресов ЛВС организации из сети Интернет;

– доступности к ресурсам ЛВС организации изнутри.

Требуемый уровень показателя качества СМИБ по предотвращению рисков ИБ – вероятность предотвращения риска несанкционированного доступа к базе данных организации (например, потеря конфиденциальности, целостности и доступности) $U_T = p_T \geq 0{,}95$, исходное состояние $U_0 = p_0 = 0{,}5$.

Таблица

Значения показателя качества, полученные на этапах проверки

a_i	0,8	0,9	0,94	0,98
θ_i	0,04	0,03	0,02	0,01

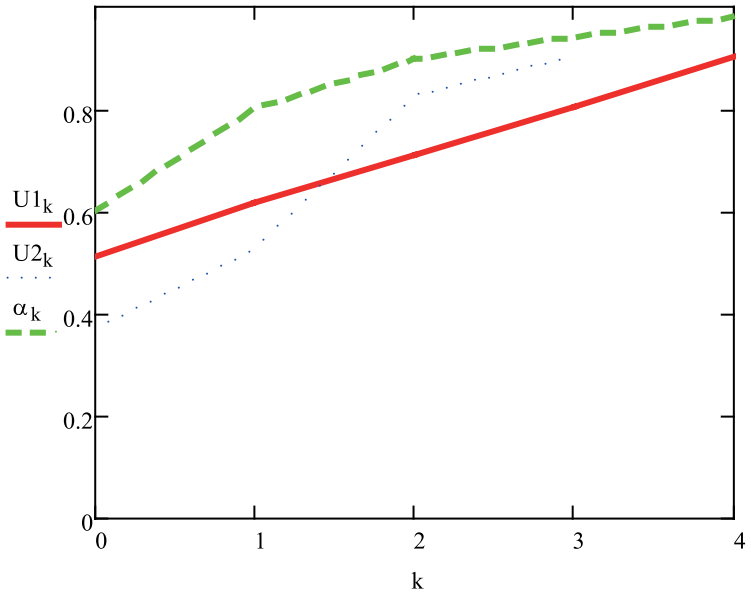

Рис. 3. Динамика роста показателя качества (*U*1 – рассчитанная без оптимизации, *U*2 – полученная в процессе оптимизации, α – значения, полученные на этапах проверок)

После решения задачи оптимизации распределения времени по проводимым мероприятиям (таблица) получены значения точек перехода от одного мероприятия к другому $p_1 = p_2 = 0{,}5$; $p_2 = p_3 = 0{,}82$; $p_3 = p_4 = 0{,}9$ (рис. 3). Согласно полученным данным рост показателя качества после оптимизации максимален, к началу четвертого этапа проверки достигнут уровень $p_4 = 0{,}9$ (планируемый $p_3 = 0{,}79$), тем самым требуемый уровень эффективности U_T может быть достигнут за меньшее время.

ЗАКЛЮЧЕНИЕ

Современная система менеджмента информационной безопасности представляет собой сложную техническую систему [12, 13], которая постоянно совершенствуется для успешного решения задач по обеспечению информационной безопасности. Усложнение системы менеджмента информационной безопасности приводит к необходимости совершенствования научно-методического аппарата аудита данных систем [14, 15]. Предложенная методика позволяет на основе модели динамики показателя качества системы менеджмента информационной безопасности осуществлять оптимальное распределение временных и материальных ресурсов по этапам аудита при планировании мероприятий аудита СМИБ.

Особенностью подхода, предлагаемого авторами, является использование не только априорных, но и апостериорных данных при начальном планировании аудита, а также для корректировки плана после каждого мероприятия аудита. Это позволяет оптимизировать использование ресурса аудита в соответствии с выбранными критериями.

По результатам проведенного вычислительного эксперимента на основе предложенной методики возможно снижение временных (стоимостных) затрат аудита на 10–15% или, соответственно, повышение качества получаемых оценок за счет рационального распределения ресурса аудита, по отношению к общеизвестным методикам планирования аудита.

Литература

1. ISO/IEC 27000:2013. Information security management systems. Overview and vocabulary (Система менеджмента информационной безопасности. Общий обзор и терминология). Международный Стандарт. Первое издание. 2013-01-14. – 25 с.
2. ISO/IEC 19011:2011. Руководство по аудиту систем менеджмента. Международный Стандарт. Второе издание. 2011-11-11. – 44 с.
3. *Аксенов В.В.* Аудит системы менеджмента информационной безопасности. Руководство. 2012 г. [Электронный ресурс]. – Режим доступа: http://itsec.by/, свободный. – Загл. с экрана.
4. ISO/IEC 27007:2011. Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по аудиту систем менеджмента информационной безопасности. Международный Стандарт. Первое издание. 2011-11-14. – 27 с.
5. *Мартыщенко Л.А., Ивченко В.П., Монастырский М.Л.* Теоретические основы информационно-статистического анализа сложных систем. – СПб: Лань, 1997. – 320 с.
6. *Астахов А.М.* Искусство управления информационными рисками. – М.: ДМК-Пресс, 2010. – 314 с.
7. ГОСТ Р 51897–2011. Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введ. 01.12.2012. М.: Госстандарт России. – 16 с.
8. ISO/IEC 31000:2009 Риск Менеджмент – Принципы и руководства. Международный Стандарт. Первое издание. 2009-11-15. – 32 с.
9. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введ. 30.11.2011. – М.: Госстандарт России. – 51 с.
10. *Гвоздев А.В., Зикратов И.А., Лебедев И.С., Лапшин С.В.,* Соловьев И.Н. Прогнозная оценка защищенности архитектур программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 126–130.
11. *Лебедев А.Н., Куприянов М.С., Недосекин Д.Д., Чернявский Е.А.* Вероятностные методы в инженерных задачах: Справочник. – СПб: Энергоатомиздат. Санкт-Петербургское отделение, 2000. – 333 с.
12. *Зикратов И.А., Одегов С.В.* Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.
13. ISO/IEC 27001:2013. Information security management systems. Requirements. Система менеджмента информационной безопасности. Требования. Международный Стандарт. Первое издание. 2013-09-25. – 23 с.
14. ГОСТ Р ИСО/МЭК 27004–2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Введ. 01.01.2012. – М.: Госстандарт России. – 62 с.
15. ГОСТ Р ИСО/МЭК 27006–2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введ. 30.09.2009. – М.: Госстандарт России. – 40 с.