ISSN 1814-1196
Научный вестник НГТУ
том 65, № 4, 2016, с. 100–109

http://journals.nstu.ru/vestnik
Science Bulletin of the NSTU
Vol. 65, No. 4, 2016, pp. 100–109

УДК 004.056:681.518

Методика оценки требуемого уровня защищенности информационных ресурсов автоматизированных систем обработки информации и управления*

Н.В. ДАВИДЮК

414056, РФ, г. Астрахань, ул. Татищева, 16, Астраханский государственный технический университет, доцент, кандидат технических наук. E-mail: davidyuknv@bk.ru

В статье представлена поэтапная методика получения количественной оценки требуемого уровня обеспечения безопасности информационных ресурсов, циркулирующих в автоматизированных системах обработки информации и управления, с привлечением экспертных групп. Существующий подход к агрегированию требований по защищенности информационных ресурсов на основе учета и первостепенного обеспечения ее конфиденциальности (секретности), в то время как требования к обеспечению целостности и доступности информации учитываются среди общих требований к автоматизированным системам обработки этих данных лишь косвенно, на практике не всегда себя оправдывает. Следовательно, вопросы получения количественной оценки требуемого уровня защищенности информационных ресурсов в рамках автоматизированных систем обработки информации и управления с учетом промежуточного оценивания степени критичности нарушения того или иного свойства информационной безопасности по-прежнему актуальны. Предложенная автором процедура подразумевает подробный анализ и декомпозицию исследуемой информационной системы на звенья, обеспечивающие функции или участвующие в обработке, хранении, передаче информационных ресурсов системы. Кроме того, в рамках методики в процессе анализа обрабатываемой информации осуществляется учет ее ценности, а также основных свойств информационной безопасности: степени критичности нарушения ее целостности, доступности и конфиденциальности для функционирования всей автоматизированной системы обработки информации и управления или для собственника. Описанная методика может применяться на практике в организациях любого масштаба в виде самостоятельной процедуры либо в составе мероприятий на этапах предварительного анализа систем обработки информации перед внедрением или совершенствованием подсистем их безопасности.

Ключевые слова: оценка уровня защищенности, показатель требуемого уровня защищенности, информационная безопасность, автоматизированная система обработки информации и управления, экспертная оценка, целостность информации, конфиденциальность информации, доступность информации

DOI: 10.17212/1814-1196-2016-4-100-109

* *Статья получена 22 ноября 2016 г.*

ВВЕДЕНИЕ

При решении вопросов обеспечения безопасности автоматизированных систем обработки информации и управления (АСОИУ), а также циркулирующих в них информационных ресурсов неизбежно возникает задача определения требований к защите конкретной информации, ее носителей, процессов обработки и их количественной оценки. Решение данной задачи является критичным для функционирования АСОИУ и лежит в основе последующих мер по внедрению вновь созданной или совершенствованию уже эксплуатируемой системы защиты информации.

Сложившийся подход к формированию требований по защищенности информации на основе рассмотрения и приоритетного обеспечения ее конфиденциальности (секретности), в то время как требования к обеспечению целостности и доступности информации фигурируют среди общих требований к системам обработки этих данных лишь косвенно, изжил себя. Ошибочно считать, что в случае ограниченного доступа узкого круга доверенных лиц к информационным ресурсам АСОИУ вероятность их искажения, хищения и уничтожения незначительна.

Кроме того, на практике в ряде случаев приоритетность обеспечения свойств безопасности информации может быть иной. К примеру, для некоторых платежных документов самым важным является свойство их целостности (достоверности, неискаженности). Затем по степени важности следует свойство доступности (потеря платежного документа или задержка платежей могут иметь материальные последствия). Требования к обеспечению конфиденциальности отдельных платежных документов могут не предъявляться вообще [1–3].

Поэтому задача получения количественной оценки требуемого уровня защищенности информационных ресурсов в рамках АСОИУ с учетом промежуточного оценивания степени критичности нарушения того или иного свойства информационной безопасности не теряет своей актуальности [4].

ПОСТАНОВКА И РЕШЕНИЕ ЗАДАЧИ

Ставится задача: необходимо получить количественную оценку требуемого уровня защищенности информационных ресурсов в рамках некоторой АСОИУ $P_{\text{о}}^{\text{общ}}$.

Для решения данной задачи предлагается методика, состоящая из следующих основных этапов.

1. Предварительный анализ АСОИУ и информационных ресурсов, циркулирующих в ней, с целью получения исходных данных:

- перечня выделенных в АСОИУ узлов и звеньев $З_i$, $i = 1,\ldots, s$, s – общее количество звеньев АСОИУ;
- перечня информационных ресурсов, обрабатываемых АСОИУ, – общего и поузлового;

2. Ранжирование узлов и звеньев АСОИУ по группам согласно ценности информационных ресурсов, обрабатываемых ими.

3. Получение количественной оценки требуемого уровня защищенности информационных ресурсов АСОИУ $P_{\text{о}}^{\text{общ}}$ с учетом их ценности и степени

критичности нарушения целостности, доступности и конфиденциальности информации.

На первом этапе необходимо декомпозировать исследуемую АСОИУ на ключевые узлы, в качестве которых выделим следующие группы:

1) рабочие места и терминалы;

2) серверы и сетевое оборудование;

3) коммуникационное оборудование, в том числе физические каналы передачи информации, линии связи;

4) устройства ввода/вывода информации, преобразования первичной измерительной информации и управления;

5) вспомогательные устройства, обеспечивающие функционирование АСОИУ, включая системы основного и резервного питания, вентиляции и т. д.

При необходимости выделенные узлы АСОИУ поддаются дальнейшей декомпозиции. Например, группа 4 может быть уточнена по конкретным видам устройств ввода/вывода, датчикам системы, типам их чувствительных элементов; группа 2 – по платформам, на которых функционируют серверы и т. д.

Особое внимание в АСОИУ необходимо уделять каналам передачи информации, поскольку зачастую несанкционированное воздействие на информационный ресурс связано с получением непосредственного или контактного доступа к ним.

При этом каналы передачи отличает от остальных выделенных звеньев АСОИУ распределенный характер, что обусловливает специфику обеспечения защищенности передаваемой информации. При необходимости учета указанной специфики предлагается следующий способ: на основе сведений о геометрических особенностях объекта информатизации и схемы расположения на нем звеньев АСОИУ представить защищаемый физический канал передачи информации совокупностью линейных участков, каждый из которых рассматривать в качестве отдельного звена АСОИУ. Таким образом, и для распределенных звеньев АСОИУ справедливы положения, изложенные ниже (см. также [5, 6]).

На втором этапе возникает локальная задача распределения выделенных на первом этапе информационных ресурсов АСОИУ и звеньев, участвующих в их обработке, по степени важности обеспечения безопасности в зависимости от их ценности.

На практике ценность любого информационного ресурса определяется средней величиной потенциального ущерба в случае нарушения информационной безопасности угрозой заданного типа. Ущерб от потери (искажения, модификации, уничтожения) информации, в свою очередь, жестко коррелирует с ее стоимостью для собственника, которая в общем случае определяется затратами на ее получение, а также зависит от выбора путей получения информации и минимизации затрат при добывании необходимых сведений выбранным путем.

В рамках АСОИУ циркулируют следующие виды информационных ресурсов:

- служебная информация, необходимая для функционирования АСОИУ и системы ее защиты;

• информация, которая обрабатывается, хранится, передается в контуре АСОИУ и не относится к служебной.

Один из подходов к классификации служебной информации АСОИУ приведен в работе [7]:

• особо важные информационные ресурсы – незаменимая информация, имеющая высокую ценность и необходимая для функционирования АСОИУ;

• важная информация – информация, которая может быть заменена или восстановлена в случае утраты, но процесс восстановления трудоемок или связан с большими временными или финансовыми затратами и имеет относительно высокую ценность;

• полезная информация – информация, имеющая средний уровень ценности и трудно восстанавливаемая, однако ее кража или искажение не окажутся критичными для функционирования АСОИУ;

• несущественная информация – информация, не представляющая особой ценности для эффективного функционирования АСОИУ.

Отметим, что несанкционированная модификация или уничтожение несекретной информации (изменение команд управления и др.) может повлечь серьезные последствия в функционировании АСОИУ, поэтому нельзя пренебрегать учетом так называемых несущественных информационных ресурсов при обеспечении безопасности АСОИУ.

Информация, обрабатываемая АСОИУ, но не относящаяся к служебной, содержит сведения организации секретного или конфиденциального характера, перечень которых, как и аспекты, касающиеся формирования указанного перечня, определен в соответствующих законодательных актах [8–11].

В то время как классификация и система грифования секретной информации жестко регламентированы, классификация конфиденциальной информации по ценности обычно осуществляется ее владельцем с привлечением экспертной группы в удобной для конкретной организации системе градаций.

Для унификации в рамках работы положим, что на основе предварительной оценки потенциального ущерба от потерь, модификации или уничтожения информационных ресурсов АСОИУ принята их классификация, аналогичная служебной информации АСОИУ:

• особо важная информация;

• важная информация;

• информация средней важности;

• информация низкой важности.

С целью ранжирования выделенных звеньев АСОИУ по степени важности обеспечения их безопасности введем показатель ценности информационных ресурсов $Q_i^{\text{ц}}$, обрабатываемых *i*-м звеном АСОИУ. Как указывалось выше, оценку указанного показателя целесообразно проводить неформальными методами – с привлечением экспертной группы. В дальнейшем обработка полученной экспертной информации может производиться любыми известными методами [12].

На основании перечня информационных ресурсов АСОИУ и заданной шкалы оценок эксперты должны оценить стоимость *j*-го информационного ресурса C_j, циркулирующего в системе.

В случае затруднений в получении от эксперта конкретной численной оценки возможно предложение некого стоимостного диапазона и переход к относительным показателям:

$$C_j = \frac{C_j^{\min}\gamma_1 + C_j^{\max}\gamma_2}{(\gamma_1 + \gamma_2)\left(C_j^{\min} + C_j^{\max}\right)}, \tag{1}$$

где γ_1 и γ_2 – эмпирические коэффициенты; $j = 1,\ldots, m$, m – общее количество выделенных информационных ресурсов АСОИУ.

Тогда показатель ценности j-го информационного ресурса АСОИУ

$$q_j^{\text{ц}} = \frac{C_j}{\max\limits_j C_j}. \tag{2}$$

Показатель ценности информационных ресурсов для конкретного i-го узла АСОИУ $З_i$ определяется как

$$Q_i^{\text{ц}} = \max_{j \in З_i} q_j^{\text{ц}}, \tag{3}$$

где $q_j^{\text{ц}}$ – ценность j-го информационного ресурса АСОИУ.

В результате получаем обобщенную матрицу показателей ценности информационных ресурсов $Q^{\text{ц}}$ для всех выделенных звеньев $З_i$ рассматриваемой АСОИУ, $i = 1,\ldots, s$, s – общее количество звеньев АСОИУ:

$$Q^{\text{ц}} \quad \begin{matrix} З_1 \\ З_i \\ З_s \end{matrix} \begin{pmatrix} Q_1^{\text{ц}} \\ Q_i^{\text{ц}} \\ Q_s^{\text{ц}} \end{pmatrix}. \tag{4}$$

Полученная матрица (4) позволяет ранжировать звенья АСОИУ согласно ценности обрабатываемых на них информационных ресурсов по группам: особо важные, важные, средней и низкой важности.

Перейдем к третьему этапу. Для оценки искомого показателя требуемого уровня защищенности информационных ресурсов АСОИУ $P_{\text{о}}^{\text{общ}}$ введем понятие степени критичности информационных ресурсов $Q_i^{\text{к}}$ i-го звена АСОИУ.

Поскольку информационная безопасность АСОИУ заключается в обеспечении совокупности таких базовых характеристик обрабатываемой инфор-

мации, как конфиденциальность, целостность и доступность [13, 14], показатель $Q^{к}$ должен учитывать количественные оценки степени критичности нарушения указанных свойств для каждого выделенного узла и звена АСОИУ.

В результате обработки экспертной информации получим сводную матрицу оценок критичности $Q^{к}$ вида

$$\begin{array}{c} \quad Q^{к}_{конф} \quad Q^{к}_{дост} \quad Q^{к}_{цел} \\ \begin{array}{c} З_1 \\ З_i \\ З_s \end{array} \begin{pmatrix} q^{1}_{конф} & q^{1}_{дост} & q^{1}_{цел} \\ q^{i}_{конф} & q^{i}_{дост} & q^{i}_{цел} \\ q^{s}_{конф} & q^{s}_{дост} & q^{s}_{цел} \end{pmatrix}, \end{array} \qquad (5)$$

где $З_i$ – i-е звено АСОИУ, $i = 1,\ldots, s$, s – общее количество звеньев АСОИУ; $q^{i}_{конф} = [0-1]$, $q^{i}_{дост} = [0-1]$, $q^{i}_{цел} = [0-1]$ – коэффициенты степени нарушения свойств информационной безопасности (конфиденциальности, доступности и целостности соответственно) для $З_i$, заданные на диапазоне [0…1] и полученные в результате обработки экспертной информации на основании предварительного анализа АСОИУ на первом этапе методики.

При этом степень согласованности экспертов оценивается известными методами (например, вычисление коэффициента конкордации и подтверждение статистической значимости экспертизы с применением χ^2-распределения) [15].

Поскольку непосредственная численная оценка показателей нарушения информационной безопасности на практике часто весьма трудоемка и затруднительна, возможно проведение описанной экспертной процедуры с введением системы интервальных или лингвистических (качественных) оценок. Также можно упростить задачу, требуя от эксперта диапазон, в котором, по его мнению, находится искомая величина. Эксперт указывает верхнюю и нижнюю границы этого диапазона, а при обработке результатов можно использовать среднее значение полученных величин:

$$q_i = \frac{q_i^{\min} + q_i^{\max}}{2}, \qquad (6)$$

где $q_i^{\min}$ – нижняя граница диапазона значений параметра, данная экспертом; $q_i^{\max}$ – верхняя граница диапазона значений параметра, данная экспертом.

В силу различной важности звеньев АСОИУ по обрабатываемой ими информации механизмы оценки искомых показателей $P_{о}$ для выделенных групп звеньев также должны различаться.

Для групп важных $З_{в}$ и особо важных звеньев $З_{ов}$ АСОИУ при формировании показателей $P_{о}^{З_{в}}$ и $P_{о}^{З_{ов}}$ следует использовать мультипликативную

свертку найденных показателей $Q^{к}_{конф}$, $Q^{к}_{дост}$, $Q^{к}_{цел}$, поскольку вклад каждого из них в общую оценку чрезвычайно критичен:

$$P_{о}^{З_{ов}} = \sqrt[s_{ов}]{\prod_{i=1}^{s_{ов}} \frac{\left(q^{i}_{конф} + q^{i}_{дост} + q^{i}_{цел}\right)}{3}}, \tag{7}$$

$$P_{о}^{З_{в}} = \sqrt[K]{\prod_{i=1}^{s_{в}} \left(\frac{\left(q^{i}_{конф} + q^{i}_{дост} + q^{i}_{цел}\right)}{3} \right)^{K}}, \tag{8}$$

где $s_{ов}, s_{в}$ – количество звеньев АСОИУ в группах «особо важные» и «важные» соответственно; K – коэффициент, учитывающий степень чувствительности общей оценки к показателям данной группы.

При оценивании показателей $P_{о}^{З_{св}}$ и $P_{о}^{З_{нв}}$ для звеньев АСОИУ, отнесенных к группам средней $З_{св}$ и низкой важности $З_{нв}$, используем аддитивную свертку оценок:

$$P_{о}^{З_{св}} = \sqrt{\frac{\sum_{i=1}^{s_{св}} \left(\frac{(q^{i}_{конф} + q^{i}_{дост} + q^{i}_{цел})}{3} \right)^{2}}{s_{св}}}, \tag{9}$$

$$P_{о}^{З_{нв}} = \frac{\sum_{i=1}^{s_{нв}} \left(\frac{q^{i}_{конф} + q^{i}_{дост} + q^{i}_{цел}}{3} \right)}{s_{нв}}. \tag{10}$$

Тогда обобщенный показатель требуемого уровня защищенности для информационных ресурсов АСОИУ $P_{о}^{общ}$ с учетом весов каждой группы показателей определим как

$$P_{о}^{общ} = W_{ов} P_{о}^{З_{ов}} + W_{в} P_{о}^{З_{в}} + W_{п} P_{о}^{З_{св}} + W_{н} P_{о}^{З_{нв}}, \tag{11}$$

где $\sum_{i} W_i = 1$.

ЗАКЛЮЧЕНИЕ

Таким образом, результатом применения описанной методики являются количественные показатели уровня защищенности для особо важных $P_{о}^{З_{ов}}$, важных $P_{о}^{З_{в}}$, средней $P_{о}^{З_{св}}$ и низкой важности $P_{о}^{З_{нв}}$ звеньев АСОИУ (7)–(10), учитывающие ценность, а также степень критичности нарушения целостности, доступности и конфиденциальности обрабатываемой на них информации. На основе указанных показателей получен обобщенный показатель (11) требуемого уровня защищенности информационных ресурсов в рамках АСОИУ.

На практике описанная методика может найти применение в виде самостоятельной процедуры либо в составе мероприятий на этапах предварительного анализа автоматизированных систем обработки информации и управления перед внедрением или совершенствованием подсистем безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Гайкович В.Ю., Ершов Д.В.* Основы безопасности информационных технологий [Электронный ресурс]. – URL: http://telecomlaw.ru/studyguides/osn_bez_IT.pdf (дата обращения: 14.12.2016).

2. Управление информационной безопасностью / С.В. Белов, А.Н. Савельев, И.Ю. Кучин, Ш.Ш. Иксанов, А.Х. Бисалиева. – Астрахань: Сорокин Р.В., 2015. – 132 с.

3. *Ажмухамедов И.М., Князева О.М.* Унификация подходов к управлению уровнем информационной безопасности в организациях различного профиля // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 1. – С. 66–77.

4. *Космачева И.М., Сибикина И.В., Галимова Л.В.* Алгоритм оценки риска нарушения информационных сервисов в организации // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 2. – С. 58–64.

5. *Давидюк Н.В., Космачева И.М., Сибикина И.В.* Процедура оценки показателей обнаружительной способности системы безопасности для объектов информатизации // Информация и безопасность. – 2012. – № 4. – С. 537–542.

6. *Давидюк Н.В., Белов С.В.* Процедура оценки защищенности автоматизированной системы обеспечения физической безопасности объектов // Математические методы в технике и технологиях: сборник трудов XXI Международной научной конференции, Саратов, 27–31 мая 2008 г. – Саратов, 2008. – Т. 6. – С. 269–271.

7. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – 575 с.

8. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 06.03.1997 N 188 (в редакции указов Президента РФ от 23.09.2005 г. N 1111; от 13.07.2015 г. N 357) [Электронный ресурс]. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102046005 (дата обращения: 14.12.2016).

9. Об утверждении перечня сведений, отнесенных к государственной тайне: указ Президента Российской Федерации от 30.11.1995 N 1203 (с изменениями) [Электронный ресурс]. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102038480 (дата обращения: 14.12.2016).

10. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями и дополнениями) [Электронный ресурс]. – URL: http://base.garant.ru/12148567/ (дата обращения: 14.12.2016).

11. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями) [Электронный ресурс]. – URL: http://base.garant.ru/12136454/ (дата обращения: 14.12.2016).

12. *Ларичев О.И.* Теория и методы принятия решений. – М.: Логос, 2002. – 391 с.

13. *Цирлов В.Л.* Основы информационной безопасности автоматизированных систем. – М.: Феникс, 2008. – 174 с.

14. *Ажмухамедов И.М., Князева О.М.* Принципы обеспечения комплексной безопасности информационных систем // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 1. – С. 66–77.

15. *Попов Г.А., Попова Е.А., Мельников А.В.* Анализ параметров информационной безопасности автоматизированных систем на основе использования уточненных экспертных оценок // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2015. – № 1. – С. 33–39.

Давидюк Надежда Валерьевна, кандидат технических наук, доцент кафедры информационной безопасности Астраханского государственного технического университета. Основное направление научных исследований – системы физической безопасности различных объектов, в том числе и объектов информатизации. Имеет более 20 публикаций, в том числе 3 авторских свидетельства. E-mail: davidyuknv@bk.ru

The procedure of quantitative estimation of the required security level for information resources of automated information processing and management systems[*]

N.V. DAVIDYUK

Astrakhan State Technical University, 16 Tatishheva St., Astrakhan, 414056, Russian Federation, PhD (Eng.), an associate professor. E-mail: davidyuknv@bk.ru

The article presents a stepwise procedure of quantitative estimation of the required security level of information resources circulating in automated information processing and management systems with the assistance of expert groups. The current approach which proposes to aggregate requirements for the protection of information resources based on due regard to and priority of ensuring data confidentiality (privacy) is not always applicable in practice, while the requirements to ensure the integrity and availability of information are considered as general requirements for automated data-processing systems only indirectly. Therefore, the problems of obtaining quantitative estimation of the required level of information resource protection within the framework of automated information processing and management systems based on the intermediate estimation of the degree of importance of information security properties are still relevant. The proposed procedure involves a detailed analysis and decomposition of the information system under study into components that provide functions or are involved in processing, storage and transmission of information resources of the system. In addition, the method involves taking into account the value of information as well as the degree of importance of violation of its integrity, accessibility and confidentiality for the functioning of the whole automated information processing and management system or for the owner. The described method can be applied in practice in organizations of all sizes as an independent procedure or as part of the activities at the stages of preliminary analysis of information processing systems before implementing or improving their security subsystems.

Keywords: security level estimation, required security level measure, information security, automated system of information processing and management, expert evaluation, data integrity, data confidentiality, availability of information

DOI: 10.17212/1814-1196-2016-4-100-109

REFERENCES

1. Gaikovich V.Yu., Ershov D.V. *Osnovy bezopasnosti informatsionnykh tekhnologii* [The fundamentals of information technology security]. Available at: http://telecomlaw.ru/ study-guides/osn_bez_IT.pdf (accessed 14.12.2016)

2. Belov S.V., Savel'ev A.N., Kuchin I.Yu, Iksanov Sh.Sh., Bisalieva A.Kh. *Upravlenie informatsionnoi bezopasnost'yu* [Information security management]. Astrakhan', Sorokin R.V. Publ., 2015. 132 p.

3. Azhmukhamedov I.M., Knyazeva O.M. Unifikatsiya podkhodov k upravleniyu urovnem informatsionnoi bezopasnosti v organizatsiyakh razlichnogo profilya [The unification of approaches to the management of information security in organizations of various profiles]. *Vestnik Astrakhanskogo*

[*] *Received 22 November 2016.*

gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics, 2015, no. 1, pp. 66–77.

4. Kosmacheva I.M., Sibikina I.V., Galimova L.V. Algoritm otsenki riska narusheniya informatsionnykh servisov v organizatsii [The risk assessment algorithm violations in the organization of information services]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2015, no. 2, pp. 58–64.

5. Davidyuk N.V., Kosmacheva I.M., Sibikina I.V. Protsedura otsenki pokazatelei obnaruzhitel'noi sposobnosti sistemy bezopasnosti dlya ob"ektov informatizatsii [The procedure for evaluation of indicators detectability security for objects of informatization]. *Informatsiya i bezopasnost'– Information and Security*, 2012, no. 4, pp. 537–542.

6. Davidyuk N.V., Belov S.V. [The procedure of security estimating of the automated physical security system]. *Matematicheskie metody v tekhnike i tekhnologiyakh: sbornik trudov XXI Mezhdunarodnoi nauchnoi konferentsii* [Proceedings XXI International Scientific Conference "Mathematical Methods in Engineering and Technology"], Saratov, 27–31 May 2008, vol. 6, pp. 269–271.

7. Gerasimenko V.A. *Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh* [The Information secutity in automated data processing systems]. Moscow, Energoatomizdat Publ., 1994. 575 p.

8. *Ob utverzhdenii perechnya svedenii konfidentsial'nogo kharaktera:* Ukaz Prezidenta Rossiiskoi Federatsii ot 06.03.1997 N 188 (v redaktsii ukazov Prezidenta RF ot 23.09.2005 g. N 1111; ot 13.07.2015 g. N 357) [About approving the list of confidential information. Presidential Decree]. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102046005 (accessed 14.12.2016)

9. *Ob utverzhdenii perechnya svedenii, otnesennykh k gosudarstvennoi taine (s izmeneniyami)*: ukaz Prezidenta Rossiiskoi Federatsii ot 30.11.1995 N 1203 [About approval of the list of information classified as state secret (as amended). Presidential Decree]. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102038480 (accessed 14.12.2016)

11. RF Federal Law "About trade secrets" of July 29, 2004 N 98-FZ (as amended). (In Russian) Available at: http://base.garant.ru/12136454 (accessed 14.12.2016)

12. Larichev O.I. *Teoriya i metody prinyatiya reshenii* [The theory and methods of decision-making]. Moscow, Logos Publ., 2002. 391 p.

13. Tsirlov V.L. *Osnovy informatsionnoi bezopasnosti avtomatizirovannykh sistem* [The basics of information security of automated systems]. Moscow, Feniks Publ., 2008. 174 p.

14. Azhmukhamedov I.M., Knyazeva O.M. Printsipy obespecheniya kompleksnoi bezopasnosti informatsionnykh sistem [The principles of information systems complex security]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2015, no. 1, pp. 66–77.

15. Popov G.A., Popova E.A., Mel'nikov A.V. Analiz parametrov informatsionnoi bezopasnosti avtomatizirovannykh sistem na osnove ispol'zovaniya utochnennykh ekspertnykh otsenok [The analysis of information security parameters of the automated systems by using revised expert estimates]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2015, no. 1, pp. 33–39.