УДК 004.891

ОЦЕНКА ФИНАНСОВЫХ ЗАТРАТ НА ПОСТРОЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Жук А. П., Осипов Д. Л., Гавришев А. А.
Северо-Кавказский федеральный университет, г. Ставрополь, РФ
E-mail: alekszhuk@mail.ru

В статье рассмотрены системы поддержки принятия решений, ориентированные на обеспечение информационной безопасности. Установлено, что многие известные системы либо не обладают подсистемой вычисления финансовых затрат на построение средств защиты информации, либо математический аппарат, применяемый в них, отличается большой вычислительной сложностью. Авторами на основе математического аппарата теории игр был разработан метод оценки финансовых затрат на построение средств защиты информации, в том числе и технических систем охраны, с учетом их особенностей. На основе разработанного метода предложена структура системы поддержки принятия решений, оценивающая средства защиты информации, в том числе и технические системы охраны, на основе критерия минимизации финансовых затрат при известной стоимости защищаемой информации и дающая рекомендации лицу, принимающему управленческие решения.

Ключевые слова: СППР, теория игр, финансовые затраты, средства защиты информации.

Введение

В настоящее время в мире происходит увеличение случаев несанкционированного доступа третьих лиц к защищаемой информации. Так, только за 2013 г. было украдено более $ 25 млрд у частных и государственных компаний по всему миру [1]. Кроме того, в последнее время наметилась новая тенденция – участились атаки на технические системы охраны (ТСО) с нарушением их работы [2]. Исходя из этого интерес представляет анализ финансовых затрат на построение средств защиты информации (СЗИ), в том числе и ТСО, с учетом их особенностей.

Одним из возможных методов оценки финансовых затрат на построение СЗИ, в том числе и ТСО, по критерию минимизации финансовых затрат при известной стоимости защищаемой информации может быть использование систем поддержки принятия решения (СППР). Под СППР понимается система, которая направлена на аналитическое обоснование выбора вариантов управленческих решений в информационной системе лицом, принимающим решение (ЛПР) [3]. К настоящему времени известен ряд СППР, ориентированных на обеспечение информационной безопасности (ИБ) – см. таблицу 1.

Так, в [4] предлагается СППР по обеспечению безопасности персональных данных, которая базируется на основе правил и прецедентов, в [5] – СППР для защиты конфиденциальной информации предприятия. В [6] разработана интеллектуальная СППР по обеспечению ИБ компьютерных систем от атак. В [7] предлагается подход к разработке математического метода принятия решений по организационно-техническому управлению защитой информации.

Анализ недостатков систем [4-7] показывает, что в них отсутствует подсистема, которая отвечает за вычисление финансовых затрат на построение СЗИ, в том числе и ТСО, по критерию минимизации финансовых затрат при известной стоимости защищаемой информации.

В [8] представлена СППР для выработки компромиссного решения по обеспечению ИБ локальной вычислительной сети (ЛВС). Недостатком данной системы является сложность математических расчетов и затруднительность оценки денежных ресурсов, необходимых для обеспечения ИБ. Кроме того, она рассчитана на закрытые системы, к которым относятся и ЛВС, в то время как для открытых систем, например радиоканальных ТСО, рассматриваемая СППР малопригодна из-за наличия неблагоприятных факторов: погодные условия, большое расстояние передачи информации, затруднительность защиты от несанкционированного доступа на всем пути распространения радиоволн. В [9] изложена методика выбора оптимального набора программно-аппаратных СЗИ. Недостатком данной СППР является сложность математических расчетов.

Работа [10] предлагает методику синтеза оптимального варианта аппаратно-программного комплекса защиты информации, которая рассчитана на информационные системы больших компаний, включающие в себя средства вычислительной техники, системы управления базами данных и другое. Основной недостаток данной

методики – вычислительная сложность нахождения кратчайшего пути в графе альтернативных вариантов защиты в силу большого количества способов защиты.

В [11] изложена методика оценки рисков ИБ экономических информационных систем. Основным недостатком данной методики является вычислительная сложность нахождения собственных векторов и собственных значений матрицы парных отношений и субъективность экспертных оценок. В [12] предлагается методика оценки затрат на ИБ. Данная методика является подсистемой в СППР, направленной на аудит защищенности беспроводных сетей. Однако данная подсистема выдает только количественные показатели без качественных. Кроме того, она не показывает количество убытков при реализации неэффективной защиты информации.

Таким образом, анализ открытых источников показал, что исследования в области вычисления финансовых затрат на построение СЗИ и принятие управленческие решений на основании данных вычислений являются актуальными.

Целью данной работы является разработка структуры СППР, позволяющей ЛПР оценить финансовые затраты на построение СЗИ, в том числе и ТСО. В соответствии с этим задачами данной работы являются:

- разработка метода оценки финансовых затрат на построение СЗИ, в том числе и ТСО, на основе математического аппарата теории игр;
- разработка структуры СППР, оценивающей СЗИ, в том числе и ТСО, с учетом их особенностей на основе критерия минимизации финансовых затрат при известной стоимости защищаемой информации и дающей рекомендации ЛПР.

Таблица 1. Основные СППР, ориентированные на обеспечение ИБ

Название	Область применения	Используемый математический аппарат	Вычисление финансовых затрат
СППР по обеспечению безопасности персональных данных [4]	Защита персональных данных	Онтологический анализ	Отсутствует
СППР по защите информации [5]	Анализ защищенности конфиденциальной информации	Векторное представление угроз и геометрическое моделирование угроз	Отсутствует
Разработка интеллектуальной СППР [6]	Обеспечение ИБ компьютерных систем от атак	Нейронная сеть Хопфилда	Отсутствует
Разработка функциональной модели управления защитой информации [7]	Принятие решений по организационно-техническому управлению защитой информации	Морфологический метод	Отсутствует
Выбор вариантов системы информационной безопасности на основе компьютерной СППР [8]	Локальные вычислительные сети	Совокупность экономических критериев, критериев риска, оценки уровня доверия и безопасности объекта оценки	Присутствует
Синтез интегральной системы безопасности [9]	Выбор оптимального набора программно-аппаратных СЗИ	Комплекс математических моделей многокритериальной оптимизации	Присутствует
Методика синтеза оптимального варианта аппаратно-программного комплекса защиты информации [10]	Обеспечение информационной безопасности информационной системы предприятия	Теория графов	Присутствует
Методика оценки рисков информационной безопасности [11]	Экономические информационные системы	Экспертные оценки с использованием матричных вычислений	Присутствует
Модель и метод построения семейства профилей защиты для беспроводной сети [12]	Беспроводные сети	Теория вероятностей	Присутствует

Принципы разработки СППР

Для оценки финансовых затрат на построение СЗИ, в том числе и ТСО, воспользуемся математическим аппаратом теории игр. Понятие теории игр предполагает наличие двух противоборствующих сторон, которые связаны между собой платежной матрицей вида (1):

	S_1	S_2	…	S_j
A_1	p_{11}	p_{12}	…	p_{1j}
A_2	p_{21}	p_{22}	…	p_{2j}
…	...	...	…	...
A_i	p_{i1}	p_{i2}	…	p_{ij}

(1)

Для матрицы (1) определены следующие показатели [13]: $A_1, A_2, \ldots, A_i$ – виды атаки; $S_1, S_2, \ldots, S_j$ – виды защиты; X_j – вероятностная стоимость применяемого вида защиты; $p_{ij}^{з}$ – вероятность отражения атаки A_i при использовании средства защиты S_j; p_{ij}^{a} – вероятность проведения *i*-ой атаки; p_{ij}^{y} – вероятность нанесения ущерба при *i*-ой атаке и *j*-ым средстве защиты. Для данных показателей необходимо ввести также показатель Z – стоимость потенциально похищенной информации.

Условием рациональной защиты является следующее правило: стоимость СЗИ должна быть в худшем случае равна стоимости информации, похищенной при успешной реализации атаки [13]. Исходя из этого правила можно составить следующее выражение:

$$X_j = p_{ij}^{y} \times Z \ . \qquad (2)$$

Выражение (2) показывает, что в худшем случае вероятностная стоимость применяемого вида защиты должна соответствовать произведению вероятности нанесения ущерба на стоимость потенциально похищенной информации.

Представим p_{ij}^{y} через вероятность защиты и вероятности проведения атаки [13]:

$$p_{ij}^{y} = (1 - p_{ij}^{з}) \times p_{ij}^{a} . \qquad (3)$$

Далее необходимо в (2) подставить (3):

$$X_j = (1 - p_{ij}^{з}) \times p_{ij}^{a} \times Z \ . \qquad (4)$$

Составим общую вероятностную стоимость средств защиты X_0:

$$X_0 = \sum X_j . \qquad (5)$$

Если $X_0 \le Z$, то использование СЗИ стоит признать рациональным и целесообразность их применения очевидна, в противном же случае, то есть $X_0 > Z$, использование СЗИ является нерациональным и их нецелесообразно применять.

Вычислим стоимостную разницу между вероятностною стоимостью внедрения СЗИ и стоимостью потенциально похищенной информации Z_0:

$$Z_0 = Z - X_0 . \qquad (6)$$

Получение по формуле (6) отрицательного значения означает, что внедрение таких СЗИ является потенциально нерентабельным. На основании (1-6) авторами предложена структурная схема реализации СППР, изображенная на рис. 1.

Работа предложенной СППР осуществляется следующим образом. Вначале эксперт заполняет эталонную базу данных средств защиты информации (БД СЗИ) информацией об основных СЗИ с присуждение каждому СЗИ вероятностных характеристик $p_{ij}^{з}$ и p_{ij}^{a}, учитывающих виды защиты данного СЗИ и виды атаки на данное СЗИ и изображенных в виде матрицы вероятностей отражения атаки и матрицы проведения атаки. После этого ЛПР через интерфейс пользователя формирует запрос, который включает в себя заполнение шаблона с вопросами о необходимом СЗИ и ввод информации о стоимости потенциально похищенной информации. Шаблон состоит из полей, в которых представлены вопросы, по которым проводится поиск в эталонной БД СЗ.

В случае если такое СЗИ не было обнаружено, то ЛПР через интерфейс пользователя может внести информацию о нем в эталонную БД СЗИ. После того как СЗИ обнаружено, его вероятностные характеристики вместе с информацией о стоимости потенциально похищенной информации поступают в модуль вычисления, в котором на основании формулы (4) осуществляются вычисления вероятностной стоимости каждого средства защиты, по формуле (5) проводятся вычисления общей вероятностной стоимости средств защиты и по формуле (6) вычисляется стоимостная разница между вероятностной стоимостью внедрения СЗИ и стоимостью потенциально похищенной информации.

Затем информация поступает в модуль формирования решений, который выдает рекомендации о рациональности (нерациональности) СЗИ и целесообразности (нецелесообразности) их использования и о стоимостной разнице между вероятностной стоимостью внедрения СЗИ и стоимостью потенциально похищенной информации. После этого ЛПР получает количествен-

ные (общая вероятностная стоимость, стоимостная разница между вероятностной стоимостью внедрения СЗИ и стоимостью потенциально похищенной информации) и качественные показатели (рациональность (нерациональность), целесообразность использования (нецелесообразность)), и на их основании принимает управленческие решения.

Обоснование полученных результатов

Для подтверждения достоверности предлагаемой методики рассчитаем вероятностную стоимость произвольного СЗИ на основе выражений (1)-(6) с определением количественных и качественных показателей. За основу возьмем СЗИ, предложенную в [14]. В данной работе рассматривается устройство беспроводной автомобильной сигнализации, которое защищено от навязывания ложных данных за счет использования генератора случайных чисел и двух генераторов псевдослучайной последовательности (ПСП), однако не защищено от просмотра и перехвата информации.

Для обозначенных трех видов угроз (просмотр, перехват и подмена) и видов защиты от этих угроз, определяемых по каждому СЗИ отдельно, вероятности наступления событий целесообразно описать в соответствии со шкалой, предложенной в [15] (см. таблицу 2).

Таблица 2. Распределение вероятностей наступления событий

Вероятность	Название
$0 \le P_{ij} < 0{,}2$	наступление события маловероятно
$0{,}2 \le P_{ij} < 0{,}5$	средняя вероятность наступления события
$0{,}5 \le P_{ij} < 0{,}8$	вероятность наступления события выше среднего
$0{,}8 \le P_{ij} < 1$	высокая вероятность наступления события

Матрица вероятностей отражения атаки для данного устройства выглядит следующим образом (см. таблицу 3).

Таблица 3. Матрица вероятностей отражения атаки

	Защита от просмотра	Защита от перехвата	Защита от навязывания ложных данных
Просмотр	0,1	–	–
Перехват	–	0,1	–
Навязывание ложных данных	–	–	0,8

Рис. 1. Структурная схема реализации СППР

Матрица вероятностей проведения атаки для данного устройства выглядит следующим образом (см. таблица 4):

Таблица 4. Матрица вероятностей проведения атаки

	Защита от просмотра	Защита от перехвата	Защита от навязывания ложных данных
Просмотр	0,4	–	–
Перехват	–	0,4	–
Навязывание ложных данных	–	–	0,2

Согласно данным, представленным в таблице 3, имеем следующие вероятности отражения атаки:

- $p_{11}^{з} = 0{,}1$ – вероятность защиты от просмотра;
- $p_{22}^{з} = 0{,}1$ – вероятность защиты от перехвата;
- $p_{33}^{з} = 0{,}8$ – вероятность защиты от навязывания ложных данных.

Согласно данным, представленным в таблице 4, имеем следующие вероятности проведения атаки:

- $p_{11}^{a} = 0{,}4$ – вероятность просмотра;
- $p_{22}^{a} = 0{,}4$ – вероятность перехвата;
- $p_{33}^{a} = 0{,}2$ – вероятность навязывания ложных данных.

Заметим, что в соответствии с [16] $\sum p_{ij}^{з} = 1$ и $\sum p_{ij}^{a} = 1$. Далее согласно (4) получаем вероятностную стоимость каждого средства защиты, причем Z для простоты расчетов берется равным 100 у.е., где у.е. – стоимость потенциально похищенной информации в условных единицах:

$$X_1 = 36;\ X_2 = 36;\ X_3 = 4. \qquad (7)$$

Согласно (5) получаем общую вероятностную стоимость средств защиты:

$$X_0 = X_1 + X_2 + X_3 = 76. \qquad (8)$$

Таким образом, средства защиты являются рациональным при заданном $Z = 100$ у.е., их целесообразно применять, и стоимостная разница между вероятностною стоимостью внедрения СЗИ и стоимостью потенциально похищенной информации по формуле (6) составляет 24 у.е.

Заключение

На основе математического аппарата теории игр авторами разработан метод оценки финансовых затрат на построение СЗИ, в том числе и ТСО, с учетом их особенностей. На основе разработанного метода предложена структура СППР, оценивающая СЗИ, в том числе и ТСО, на основе критерия минимизации финансовых затрат при известной стоимости защищаемой информации и дающая рекомендации лицу, принимающему решения, в виде количественных и качественных показателей. Предложенный метод оценки финансовых затрат и разработанная структура СППР отличаются:

- простотой математических расчетов;
- легкостью в программной реализации;
- наличием количественных (финансовые затраты) и качественных (целесообразность применения) показателей;
- возможностью внедрения в качестве подсистемы в любую СППР, которая предназначена для решения задач ИБ.

Литература

1. В 2013 году компании потеряли $25 млрд из-за хакеров и инсайдеров // URL: http:// cybersecurity.ru/crypto/ 188933.html (д.о. 27.02.2015).
2. Веб-камера DropCam оказалась уязвимой // URL: http://ru-bezh.ru/content/ 2014/07/30/ veb-kamera-dropcam-okazalas (д.о. 27.02.2015).
3. Кравченко Т. К., Середенко Н. Н. Выделение признаков классификации систем поддержки принятия решений // Открытое образование. № 4, 2010. – С. 71-78.
4. Васильев В.И., Белков Н.В. Система поддержки принятия решений по обеспечению безопасности персональных данных // Вестник УГАТУ. Т.15, №5(45), 2011. – С. 54-65.
5. Бондарь И.В., Гуменникова А.В., Золотарев В.В., Попов А.М. Система поддержки принятия решений по защите информации «Оазис» // Программные продукты и системы. № 3, 2011. – С. 177-180.
6. Тверской А.Н. Разработка интеллектуальной системы поддержки принятия решений в задачах выявления причинно-следственных связей и нивелирования атак на компьютерную систему // Спецтехника и связь. № 3, 2011. – с. 32-40.
7. Машкина И.В., Гузаиров М.Б. Методы разработки функциональной модели управления защитой информации // Безопасность информационных технологий. № 2, 2008. – С. 105-110.
8. Гончаренко С.Н., Рагозин Ю.Н. Выбор вариантов системы информационной безопасно-

сти ЛВС на основе компьютерной системы поддержки принятия решений // Горный информационно-аналитический бюллетень. №4, 2009. – С. 117-124.
9. Хализев В.Н., Федоров С.Ю. Математическая модель синтеза интегральной системы безопасности // Научный журнал КубГАУ. № 81(07), 2012. – С. 341-350.
10. Карпов В.В. Методика синтеза оптимального варианта аппаратно-программного комплекса защиты информации от несанкционированного доступа по критерию защищенности // Программные продукты и системы. №1, 2003. – С. 36-38.
11. Тищенко Е.Н., Капустина О.А. Методика оценки рисков информационной безопасности экономических информационных систем электронной коммерции // Экономические науки. № 7(116), 2014. – С. 83-87.
12. Иващук И.Ю. Модель и метод построения семейства профилей защиты для беспроводной сети: дис. к.т.н. – СПб., 2010. – С. 133.
13. Заркумова Р. Н. Применение методов теории игр при выборе средства эффективной защиты // Сб. науч. трудов НГТУ. № 4(58), 2009. – С. 41-46.
14. Гавришев А.А., Бурмистров В.А., Анзин И.В. К вопросу об использовании псевдослучайных последовательностей для предотвращения несанкционированного доступа к радиоканалу автомобильной сигнализации // Сб. науч. трудов XI МНТК «Новые информационные технологии и системы». Пенза, ноябрь 2014. – С. 270-272.
15. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
16. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие Омск: Изд-во ОмГУ, 2013. – 160 с.

Получено 08.09.2015

Жук Александр Павлович, к.т.н., профессор Кафедры организации технологии защиты информации (ОТЗИ) Северо-Кавказского федерального университета (СКФУ). Тел. 8-918-884-14-81. E-mail: alekszhuk@mail.ru

Осипов Дмитрий Леонидович, к.т.н., доцент Кафедры ОТЗИ СКФУ. Тел. (8-865) 295-68-27. E-mail: kafotzi@gmail.com

Гавришев Алексей Андреевич, аспирант Кафедры ОТЗИ СКФУ. Тел. (8-865) 295-68-27. E-mail: kafotzi@gmail.com

ESTIMATION OF FINANCIAL COSTS FOR INFORMATION PROTECTION TOOLS DEVELOPMENT BY DECISION SUPPORT SYSTEM

Zhuk A.P., Osipov D.L., Gavrishev A.A.
North Caucasus Federal University, Stavropol, Russian Federation
E-mail: alekszhuk@mail.ru

This article examines decision support systems focused on information protection. It is found that many of known systems either are without subsystems for computing of financial costs for information protection tools development or their mathematical tools require great computing resources. We developed method for estimation of financial costs for information protection tools development including security technical systems by taking into account their specific features. Proposed method is based on the game theory mathematical tool. Based on developed method we designed structure of decision support system, which provides recommendations to manager according to results of preformed estimation of information protection tools including security technical systems. While the estimation is based on financial cost minimization criterion under known cost of protected information.

Keywords: decision support system, game theory, financial costs, information protection tools

DOI: 10.18469/ikt.2015.13.4.15

Zhuk Aleksandr Pavlovich, PhD in Technical Science, Professor of the Department of Organization of Information Security Technologies, North Caucasus Federal University, Stavropol, Russian Federation. Tel.: +79188841481. E-mail: alekszhuk@mail.ru

Osipov Dmitrij Leonidovich, PhD in Technical Science, Associate Professor of the Department of Organization of Information Security Technologies, North Caucasus Federal University, Stavropol, Russian Federation. Tel.: +78652956827. E-mail: kafotzi@gmail.com

Gavrishev Alexej Andreevich, PhD-student of the Department of Organization of Information Security Technologies, North Caucasus Federal University, Stavropol, Russian Federation. Tel.: +78652956827. E-mail: kafotzi@gmail.com

References

1. In 2013, the company lost $ 25 billion due to hackers and insiders. Available at: http://cybersecurity.ru/crypto/188933.html. (Accessed: 27.02.2015). (In Russian).
2. Webcam DropCam is vulnerable. Available at: http://ru-bezh.ru/content/2014/07/30/veb-kamera-dropcam-okazalas (Accessed: 27.02.2015). (In Russian).
3. Kravchenko T.K., Seredenko N.N. Vydelenie priznakov klassifikacii sistem podderzhki prinjatija reshenij [Classification of decision support systems]. *Otkrytoe obrazovanie*, 2010, no. 4, pp. 71-78.
4. Vasiliev V.I., Belkov N.V. Sistema podderzhki prinjatija reshenij po obespecheniju bezopasnosti personal'nyh dannyh [Decision support system security of personal data]. *Vestnik UGATU*, 2011, vol. 15, no. 5, pp. 54-65.
5. Bondar' I.V., Gumennikova A.V., Zolotarev V.V., Popov A.M. Sistema podderzhki prinjatija reshenij po zashhite informacii «Oazis» [«Oasis»: decision support system for the information security]. P*rogrammnye produkty i sistemy*, 2011, no. 3, pp. 177-180.
6. Tverskoi A.N. Razrabotka intellektual'noj sistemy podderzhki prinjatija reshenij v zadachah vyjavlenija prichinno-sledstvennyh svjazej i nivelirovanija atak na komp'juternuju sistemu [Development of intellectual decision support system in the task of identifying cause-and-effect relationships and leveling attacks on computer system]. *Spetstekhnika i svyaz'*, 2011, no. 3, pp. 32-40.
7. Mashkina I.V., Guzairov M.B. Metody razrabotki funkcional'noj modeli upravlenija zashhitoj informacii [Methods of development of a functional model of information security management]. *Bezopasnost Informatsionnykh Tekhnology*, 2008, no. 2, pp. 105-110.
8. Goncharenko S.N., Ragozin Y.N. Vybor variantov sistemy informacionnoj bezopasnosti LVS na osnove komp'juternoj sistemy podderzhki prinjatija reshenij [The choice of variants of LAN information security based on computer decision support system]. *Gorny Informatsionno-Analiticheskiy Byulleten* [Mining Informational and Analytical Bulletin], 2009, no. 4, pp. 117-124.
9. Halizev V.N., Fedorov S.Y. Matematicheskaja model' sinteza integral'noj sistemy bezopasnosti [Mathematical model for a synthesis of an integrated security system]. *Politematicheskii setevoi elektronnyi nauchnyi zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Polythematic online scientific journal of Kuban State Agrarian University], 2012, no. 81, pp. 341-350.
10. Karpov V.V. Metodika sinteza optimal'nogo varianta apparatno-programmnogo kompleksa zashhity informacii ot nesankcionirovannogo dostupa po kriteriju zashhishhennosti [Methods of synthesis of optimal variant of hardware and software to protect information from unauthorized access by the criterion of security]. *Programmnye produkty i sistemy* [Software & Systems], 2003, no. 1, pp. 36-38.
11. Tishchenko E. N., Kapustina O. A. Metodika ocenki riskov informacionnoj bezopasnosti jekonomicheskih informacionnyh sistem jelektronnoj kommercii [The methodology of assessing information security risks economic information systems e-commerce]. *Ekonomicheskie nauki*, 2014, no. 7, pp. 83-87.
12. Ivashchuk I.Yu. *Model' i metod postroeniya semeistva profilei zashchity dlya besprovodnoi seti* [The model and method for constructing a family of security profiles for the wireless network], Ph.D. Thesis, ITMO University, Saint Petersburg, Russia, 2010, 133 p.
13. Zarkumova R.N. Primenenie metodov teorii igr pri vybore sredstva jeffektivnoj zashhity [Application of game theory in choosing the means of effective protection], *Sbornik nauchnykh trudov NGTU*, 2009, no. 4, pp. 41-46.
14. Gavrishev A.A., Burmistrov V.A., Anzin I.V. K voprosu ob ispol'zovanii psevdosluchajnyh posledovatel'nostej dlja predotvrashhenija nesankcionirovannogo dostupa k radio-kanalu avtomobil'noj signalizacii [The use of pseudo-random sequences to prevent unauthorized access to the radio car alarm. New information technologies and systems], *Sbornik nauchnyh trudov XI MNTK «Novye informacionnye tehnologii i sistemy»* [Proceedings of the Eleventh International Conference of Science and Technology], Penza, Russia, November 25-27, 2014, pp. 270-272.
15. Mel'nikov V. V. *Bezopasnost' informatsii v avtomatizirovannykh sistemakh* [Security of information in automated systems]. Finansy i statistika Publ., Moscow, Russia, 2003, 368 p.
16. Guts A. K. and Vakhnii T. V. *Teoriya igr i zashchita komp'yuternykh sistem: uchebnoe posobie* [Game theory and the protection of computer systems: Textbook]. OmGU Publ., Omsk, Russia, 2013, 160 p.

Received 08.09.2015