Александр В. Кузнецов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID0000-0002-7160-1845

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМИЧЕСКОГО АППАРАТА УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ И РЕЗУЛЬТАТЫ ЕЕ ПРИМЕНЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2017.4.06

Аннотация. В настоящей статье рассматривается актуальная задача в области защиты информации, обусловленная отсутствием алгоритмического аппарата управления событиями безопасности и автоматизации процедур определения набора регистрируемых событий безопасности. В первой части статьи сформулирована постановка математической задачи, подлежащей автоматизации с использованием табличного процессора, в том числе определена целевая функция и её переменные, а также приведены ссылки на источники, содержащие сведения о самом алгоритме решения. Представлено писание предложенного автором программного модуля, реализующего алгоритм определения набора регистрируемых событий безопасности, разработанного на базе табличного процессора, сертифицированного по требованиям безопасности информации Федеральной службой по техническому и экспортному контролю. Представлено описание контрольного примера, подготовленного для тестирования разработанного программного модуля, размерностью 30х20, содержащего 14 вариантов пороговых значений количества зарегистрированных событий безопасности варьировалось. Результаты применения программного модуля подтвердили соблюдение заданных граничных условий задачи, выявили нелинейную зависимость целевой функции от увеличения количества регистрируемых событий безопасности, а также нелинейную зависимость процента регистрируемых событий безопасности от общего исходного количества событий безопасности, подлежащих регистрации на источнике событий. Оценка производительности применения предложенного программного модуля, а именно загрузки центрального процессора, являлась приемлемой (не превысила 33%), что позволяет применять данную программную реализацию для типовых автоматизированный рабочих местах специалистов по защите информации, оснащенных соответствующими табличными процессорами. Предложенный в статье подход к программной реализации различных алгоритмов может быть инвариантен к области применения.

Ключевые слова: событие безопасности, управление событиями безопасности, SIEM, источник событий, табличный процессор

Для цитирования. **КУЗНЕЦОВ, Александр В**. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМИЧЕСКОГО АППАРАТА УПРАВЛЕНИЯ СОБЫТИЯМИ БЕЗОПАСНОСТИ И РЕЗУЛЬТАТЫ ЕЕ ПРИМЕНЕНИЯ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 52-59, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/277>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.06.

Aleksandr V. Kuznetcov
Financial University under the Government of the Russian Federation(Financial University),
Leningradsky prospect, 49, Moscow, 125993, Russia
e-mail: a.kuznetsov@ntc-vulkan.ru, ORCID 0000-0002-7160-1845

Software for security event management:Development and utilization

DOI: http://dx.doi.org/10.26583/bit.2017.4.06

Abstract. We address the challenge to the information security coming from the lack of algorithmic machinery for managing the security events. We start with a mathematical formulation of the problem for a tabular processor by introducing an appropriate target function. Details of corresponding algorithm can be found by following the provided links. We describe our original software module that implements the algorithm for determining the registered security events. The module is based on the tabular processor certified by the Russian Federal Service for Technical and Export Control. We present a control sample for testing the developed module. The sample has the dimension 30x20 and contains 14 choices for threshold values of security events number. The results of the tests comply with the specified boundary conditions and demonstrate a nonlinear dependence of the objective function onthe number of registered security events, as well as a nonlinear dependence of the percentage of the detected security event on the total initial number of security events to be registered at the event source. The performance of the module specifically, the central processing unit usage is found acceptable (not exceeding 33%), which allows one to use the software for typical automated workplaces equipped with appropriate tabular processors. Our approach is universal with respect to the application areas.

Keywords: security event, security event management, SIEM, event source, tabular processor
For citation. **KUZNETCOV, Aleksandr V.** Software for security event management: Development and utilization. IT Security, [S.l.], v. 24, n. 4, p. 52-59, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/277>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.06.

Введение

Вопросы защиты информации не только не теряют своей актуальности на протяжении ряда десятилетий, но и стремительно развиваются и выходят на один из первых планов в научно-практической деятельности в последние годы. Системы управления информационной безопасностью становятся неотъемлемой частью систем управления современных организации и предприятий наравне с системами управления качеством и охраной труда. Управление событиями безопасности является одним из основополагающих процессов управления в рамках систем управления информационной безопасностью. Составной частью процесса управления событиями безопасности является регистрация событий безопасности [1-2]. Принимая во внимание, что современные источники событий, а именно программное и программно-аппаратное обеспечение, способные вести журнал аудита, имеют возможности по регистрации сотен и в ряде случаев тысяч различных событий безопасности, возникает необходимость формирования алгоритмического аппарата управления событиями безопасности и автоматизации процедур определения набора регистрируемых событий безопасности. На сегодняшний день в полном объеме данная задача не решена [3-5].

В настоящей статье рассматривается вариант программной реализации алгоритмического аппарата управления событиями безопасности в рамках системы управления информационной безопасностью с использованием табличного процессора, а также результаты работы данной программной реализации на базе контрольного примера.

Алгоритмический аппарат управления событиями безопасности

В ряде публикаций автором был предложен алгоритмический аппарат управления событиями безопасности в рамках системы управления информационной безопасностью [6,7], а именно алгоритм выбора набора регистрируемых событий безопасности E, которому однозначно соответствует набор булевых переменных e, из полного набора событий безопасности, подлежащих регистрации на источнике событий, при заданной в системе класса Security Information and Event Management (далее – SIEM-системе) базе

знаний, т.е. корреляционных правил I, и ограничении на производительность источника событий, который обращал бы в максимум целевую функцию W (1).

$$W = \sum_{j=1}^{m} I_j = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ij} \cdot e_i = \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{ij}) \cdot e_i \rightarrow \max \quad (1),$$

где:

Ij – корреляционное правило из SIEM-системы;

m – количество корреляционных правил в SIEM-системы;

n – количество событий безопасности;

bij – нормирующий коэффициент, соответствующий вхождению i-ого события безопасности ei в j-ое корреляционное правило Ij.

ei – дискретная величина, соответствующая данным из набора событий безопасности E, которые могут быть зарегистрированы источником событий.

Алгоритм основан на публикациях, посвященных решению задач поиска экстремума [8-10], а также применению табличных процессоров для автоматизации решения подобных задач [11-13].

Программная реализация

Программный модуль, реализующий предложенный алгоритм, был разработан автором на базе табличного процессора. В качестве табличного процессора выступает 64-разрядная версия программного обеспечения «MicrosoftExcel 2013», входящего в программный пакет «MicrosoftOffice профессиональный плюс 2013», сертифицированный по требованиям безопасности информации ФСТЭК России [14], далее – MicrosoftExcel.
Для инсталляции, запуска и использования на автоматизированном рабочем месте программного модуля данное место должно удовлетворять следующим требованиям [15]:

частота центрального процессора не ниже 1 ГГц;
оперативная память не менее 2 Гбайт;

свободное место на жестком диске не менее 3 Гбайт;

экран с расширением не ниже 1 024 X 576;

64-разрядная операционная система не ниже MicrosoftWindows 7.

Указываемые оператором программного модуля параметры поиска решения приведены на рисунке ниже (см. рис.1). Форма представления результатов работы программного модуля приведена на рисунке ниже (см. рис. 2).

Контрольный пример

Для тестирования программного модуля автором был подготовлен контрольный пример, содержащий следующие исходные данные:

количество событий n = 30;

количество корреляционных правил m= 20;

матрицакоэффициентов b_{ij} (в каждом корреляционном правиле участвует 3 события безопасности);

матрицакоэффициентов a_{ij} (в каждой ячейке указано случайное число в интервале от 100 до 500);

пороговое значение количества зарегистрированных событий безопасности варьировалось (14 значений), но не превышало максимального значения: 10 135 событий.

Обобщенные результаты тестирования в рамках контрольного примера представлены в таблице ниже (см. Таблица 1).

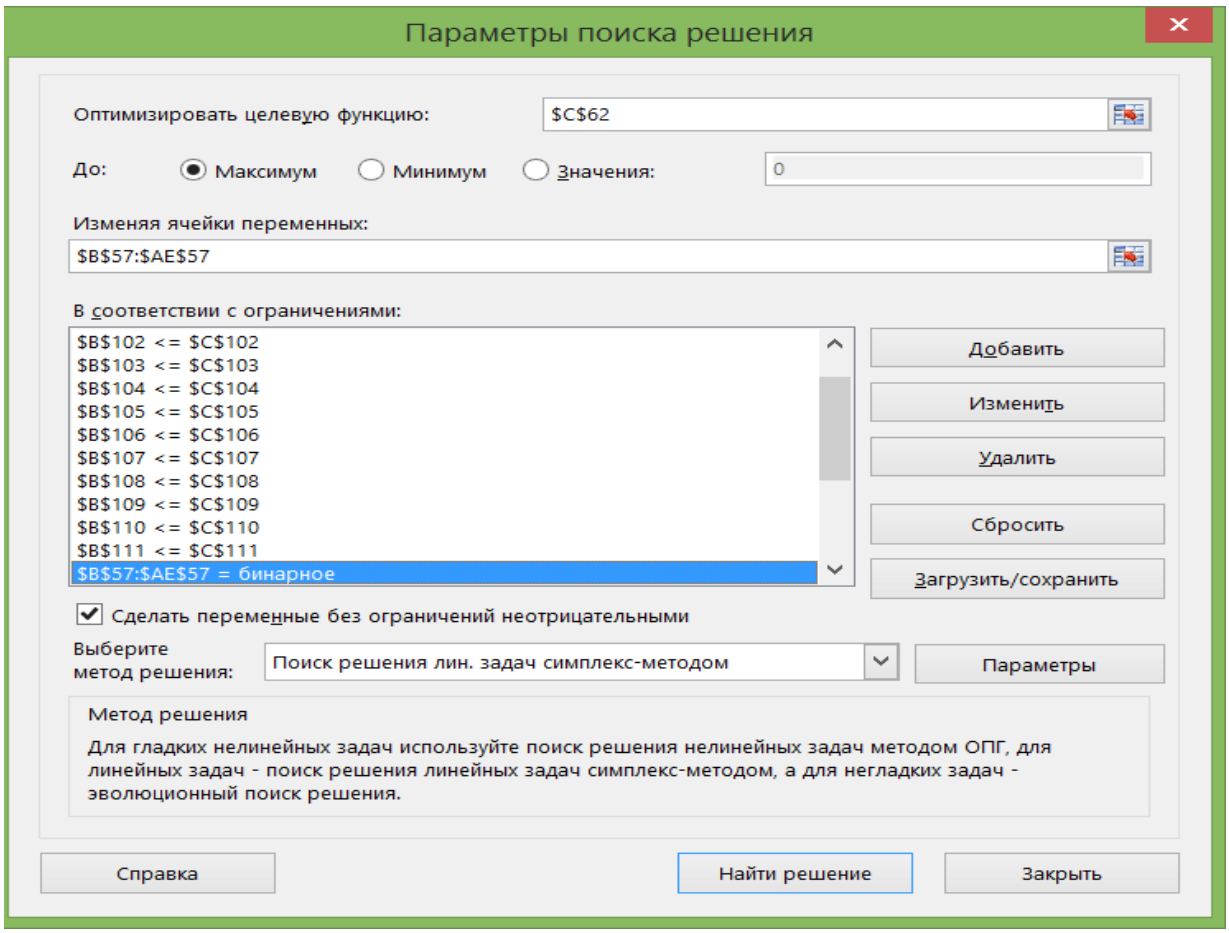

Рисунок 1 - Устанавливаемые параметры поиска решения
(Fig. 1 - Set parameters of the search decision)

Рисунок 2 - Представление результатов
(Fig. 2 - Presentation of the results)

Таблица 1. Результатытестирования в рамках контрольного примера

№ п.п.	*L*	*N*	*n*	*n/N*	*W*
1	2	3	4	5	6
1.	10 135	30	30	1,00	20
2.	10 000	30	29	0,97	18
3.	9 500	30	28	0,93	16
4.	9 000	30	27	0,90	14
5.	8 500	30	26	0,87	12
6.	8 000	30	24	0,80	10
7.	7 500	30	23	0,77	6
8.	7 000	30	21	0,70	6
9.	6 500	30	20	0,67	6
10.	6 000	30	19	0,63	5

№ п.п.	*L*	*N*	*n*	*n/N*	*W*
1	2	3	4	5	6
11.	5 500	30	17	0,57	4
12.	4 500	30	14	0,47	4
13.	3 500	30	11	0,37	2
14.	2 000	30	6	0,20	0

Зависимость *W(n)* представлена на рисунке ниже (Рисунок 3), где $W_{max} = 20$, $n_{max} = 30$.

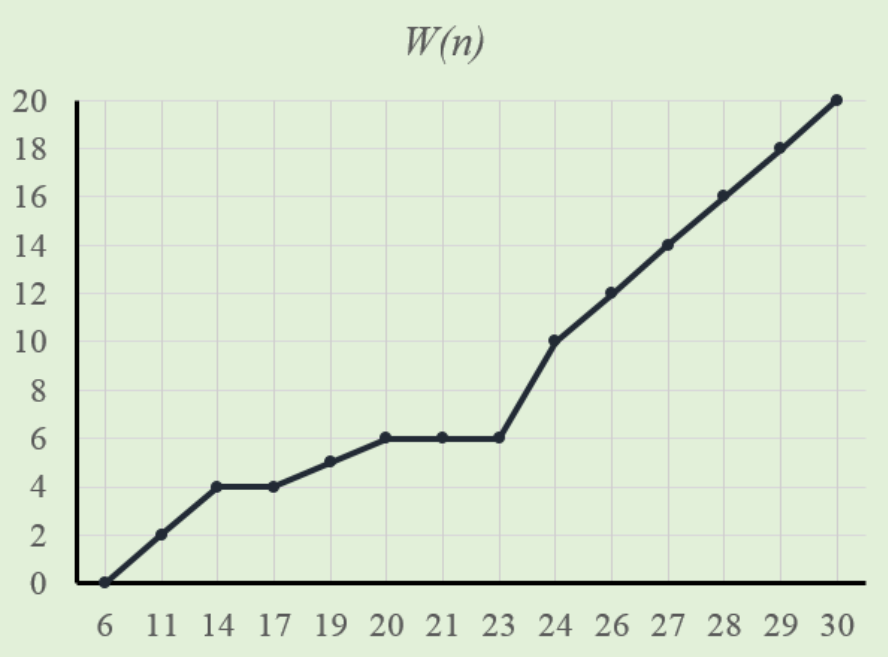

Рисунок 3 - Значения целевой функции в рамках контрольного примера
(Fig. 3 - Values of the objective function to the control example)

Зависимость *n/N(L)* представлена на рисунке ниже (Рисунок 4).

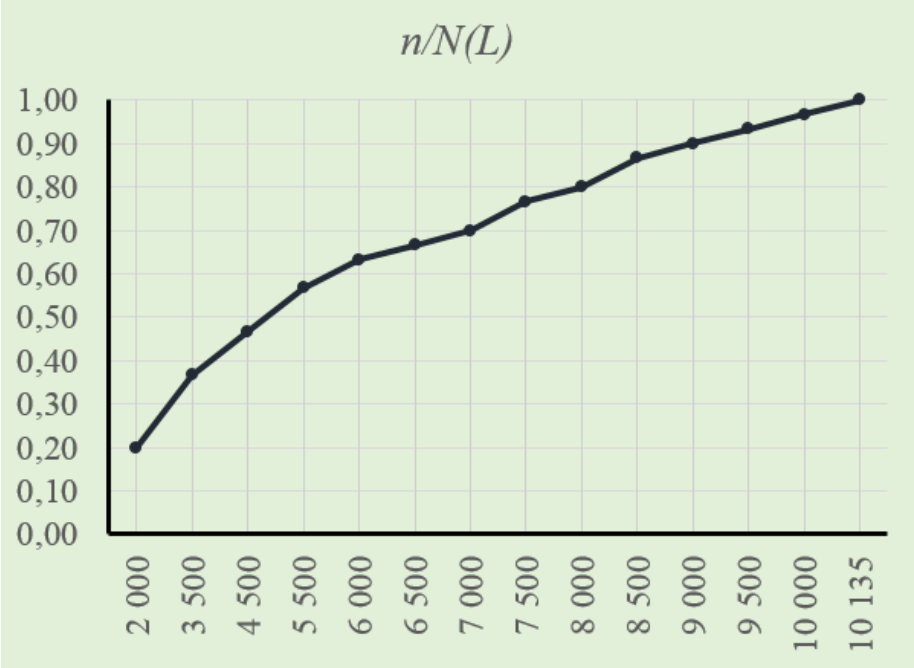

Рисунок 4 - Процент выборки событий в рамках контрольного примера
(Fig. 4 - Percentage of sampling events in the control sample)

Заключение

Результаты применения программного модуля показали, что:

выполняются граничные условия задачи, т.е. при $L = 10\,135, W = 20$, что подтверждает корректность работы алгоритма определения набора регистрируемых событий безопасности;

величина целевой функции W с увеличением количества регистрируемых событий безопасности возрастает нелинейно;

процент регистрируемых событий безопасности от общего исходного количества n/N с увеличением порогового значения L возрастает нелинейно.

При выполнении вычислений загрузка центрального процессора с IntelCorei7 с тактовой частотой 2 ГГц тестовой автоматизированной рабочей станции не превысила 33% (см. рис.5), что позволяет применять разработанную программную реализация алгоритма определения набора регистрируемых событий на типовых автоматизированный рабочих местах специалистов по защите информации, оснащенных табличным процессором MicrosoftExcel.

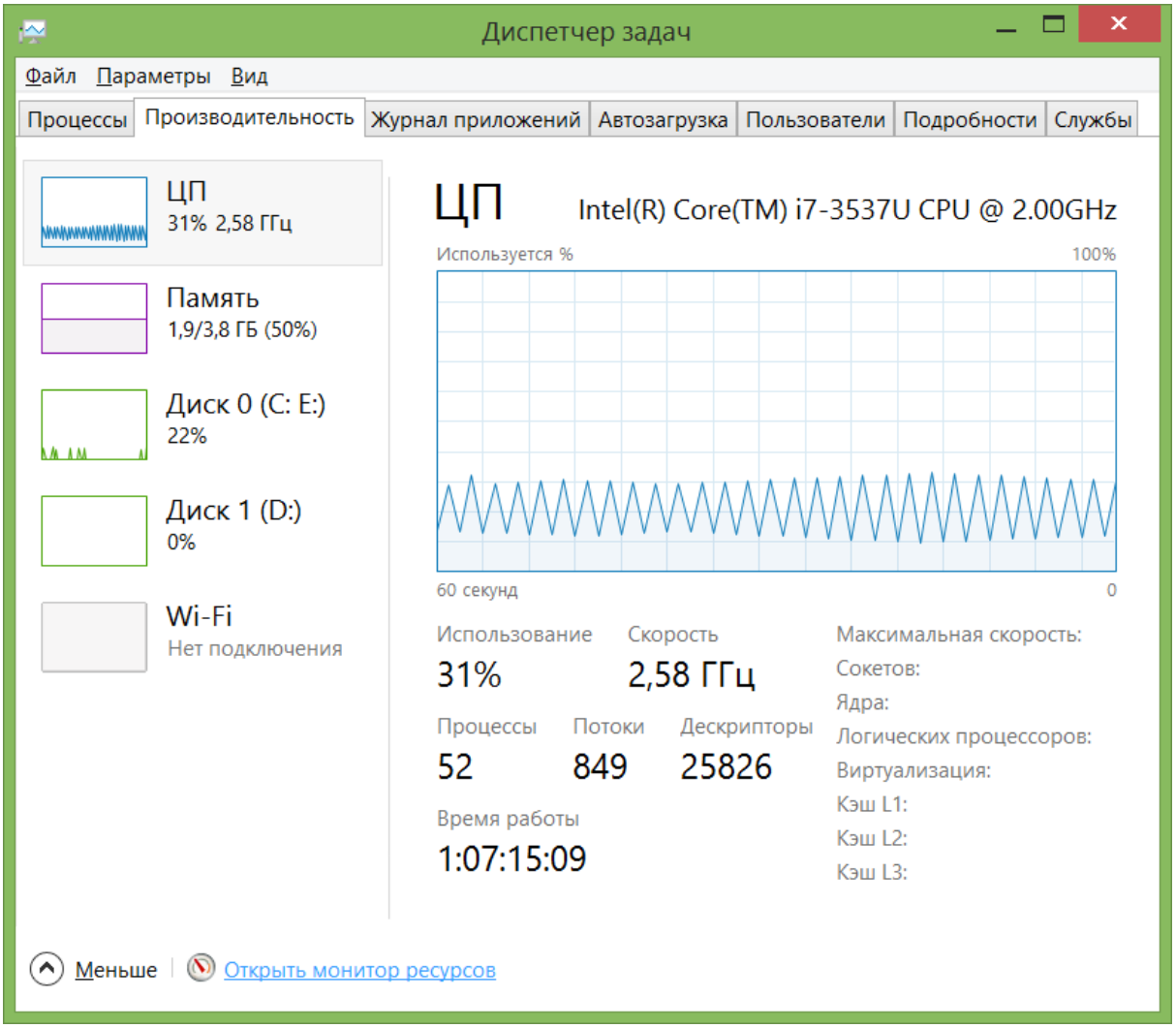

Рисунок 5 - Статистика загрузки центрального процессора при выполнении вычислений контрольного примера
(Fig. 5 - Statistics of the CPU usage while performing calculations control example)

Стоит отметить, что предложенный автором подход к программной реализации алгоритмов решения задач поиска экстремума является инвариантным к области его применения, что позволяет применять его специалистам в различных областях и сферах науки и жизнедеятельности.

СПИСОК ЛИТЕРАТУРЫ:

1 Кузнецов, А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия [Текст] А.В. Кузнецов. Вопросы защиты информации. - 2015. - N 2. - С.57–62.
2 ITILServiceOperation [Текст]: secondedition. - AXELOS. - 2011. - С.58-72.
3 Roer, K. BuldingaSecurityCulture [Текст] K. Roer. - IT Governance Publishing. – 2015. - 74 p.
4 Журналирование событий на маршрутизаторе Cisco (cisco log syslog aaa accounting snmp monitoring) [Электронный ресурс]. – Режим доступа: http://www.opennet.ru/base/cisco/cisco_logging.txt.html
5 Oltsic, J. An Analytics-based Approach to Cybersecurity [Текст] J. Oltsic. - The Enterprise Strategy Group, Inc. - 2015, may. - 4 p.
6 Кузнецов, А.В. Способ определения регистрируемых событий [Текст]. А.В. Кузнецов Вопросы кибербезопасности. - 2015. - N 5 (13). - С.23-25.
7 Кузнецов, А.В. Способ определения событий, регистрируемых в журналах аудита [Текст]. А.В. Кузнецов Безопасность информационных технологий (IT Security). ISSN 2074-7128. - М., Том 23, N 1(2016). - С.59-63.
8 Вентцель, Е.С. Исследование операций: задачи, принципы, методология [Текст]: 2-е изд. Е.С. Вентцель. - М: Наука. - 1988. - С.80-81.
9 Сигал, И.Х. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы [Текст] И.Х. Сигал, А.П. Иванова. - М: ФИЗМАТЛИТ. - 2002. - С.19, 22-25.
10 Nurminski, E.A. Single-projection procedure for linear optimization. Journal of Global Optimization [Текст] E.A. Nurminski DOI: 10.1007/s10898-015-0337-9. - 2015. - С.1-3.
11 Smith, N. Linear Programming Using Excel [Текст] N. Smith. - 2010. - С.1-7.
12 Данилин, Г.А. Математическое программирование с EXCEL [Текст]: учеб. пособие для студентов всех спец-й МГУЛа Г.А. Данилин. - М: [МГУЛ], 2005. - С.11-15.
13 Гераськин, М.И. Линейное программирование. Выполнение расчетов в табличном процессоре Excel [Текст]: учеб. пособие М.И. Гераськин. – Самара: Изд-во Самар. гос. аэрокоун-та. - 2012. - С.74-88
14 Сертифицированные продукты Microsoft [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/ru-ru/securitycertification/products.aspx.
15 Требования к системе для Office 2013 [Электронный ресурс]. – Режим доступа: https://technet.microsoft.com/ru-ru/library/ee624351.aspx.

REFERENCES:

[1] Kuznecov, A.V. Method of organization of the event management process, in terms of their treatment in the framework of information security management of the enterprise. Voprosy zashhity informacii. - 2015. - N 2. - P.57–62. (in Russian)
[2] ITIL Service Operation: second edition. - AXELOS. - 2011. - P.58-72.
[3] Roer, K. Bulding a Security Culture. K. Roer. - IT Governance Publishing. – 2015. - 74 p.
[4] Cisco log syslog aaa accounting snmp monitoring. Available at: http://www.opennet.ru/base/cisco/cisco_logging.txt.html.
[5] Oltsic, J. An Analytics-based Approach to Cybersecurity. J. Oltsic. - The Enterprise Strategy Group, Inc. - 2015, may. - 4 p.
[6] Kuznecov, A.V. The method of determining the recorded events. Voprosy kiberbezopasnosti. - 2015. - N 5 (13). - P.23-25. (in Russian).
[7] Kuznecov, A.V. The method of determining the events recorded in the audit logs. Bezopasnost' informacionnyh tehnologij (IT Security). ISSN 2074-7128. - M., v.23, N1(2016). - P.59-63. (in Russian).
[8] Ventcel', E.S. Operations research: tasks, principles, methodology: 2-e izd. E.S. Ventcel'. - M: Nauka. - 1988. - P.80-81. (in Russian).
[9] Sigal, I.H. Introduction to applied discrete programming: models and computing algorithms. I.H. Sigal, A.P. Ivanova. - M: FIZMATLIT. - 2002. - P.19, 22-25. (in Russian)
[10] Nurminski, E.A. Single-projection procedure for linear optimization. Journal of Global Optimization. E.A. Nurminski. DOI: 10.1007/s10898-015-0337-9. - 2015. - P.1-3.
[11] Smith, N. Linear Programming Using Excel. N. Smith. - 2010. - P.1-7.
[12] Danilin, G.A. Mathematical programming with EXCEL [Tekst]: ucheb. posobie dlja studentov vseh spec-j MGULa G.A. Danilin. - M: [MGUL], 2005. - P.11-15. (in Russian).
[13] Geras'kin, M.I. Linejnoe programmirovanie. Vypolnenie raschetov v tablichnom processore Excel: ucheb. posobie M.I. Geras'kin. – Samara: Izd-vo Samar. gos. ajerokoun-ta. - 2012. - P.74-88 (in Russian).

[14] Certified Microsoft products. Available at: https://www.microsoft.com/ru-ru/securitycertification/products.aspx.
[15] System requirements for Office 2013. Available at: https://technet.microsoft.com/ru-ru/library/ee624351.aspx.

Поступила в редакцию - 29 июня 2017 г. Окончательный вариант – 12 ноября 2017 г.
Received – June 29, 2017. The final version – November 12, 2017.