УДК 004.056: 519.852.61

А.С. Шабуров, Е.Е. Журилова

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

МОДЕЛЬ ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ СИМПЛЕКС-МЕТОДА

Рассмотрены тенденции развития современных технологий обработки и передачи информации, а также обусловленные этим актуальные угрозы информационной безопасности. Приведены особенности реализации компьютерных атак на корпоративные сети, обоснованы особенности бизнес-процессов обработки информации, порождающие каналы утечки информационных ресурсов. Обусловлены наиболее эффективные способы предотвращения утечки информации, посредством контроля потоков данных с использованием DLP-систем и технологий. Приведены данные практического опыта противодействия каналам утечек информации, что позволило сформировать базовые принципы борьбы с данным явлением, а также сформулировать базовые группы критериев оценки их эффективности. При этом среди основных факторов для выбора DLP-решения находится фактор количественного выявления каналов утечки информации. Приведена статистика распределения вероятностей реализаций наиболее актуальных угроз информационной безопасности за последний период. Сделаны выводы о характерных изменениях статистических данных. Приведено краткое описание симплекс-метода, используемого как основа построения модельного представления. Сформулирована задача построения математической модели. На основании статистических данных с использованием симплексного метода разработана математическая модель, описывающая изменение вероятности реализаций утечек информации по различным каналам. При этом учтены тенденции роста объемов информационных ресурсов корпоративных систем. Основываясь на полученных данных, выявлены два наиболее актуальных канала утечки на исследуемый период, даны прогнозы развития ситуации. Определена возможность DLP-систем по контролю каналов утечки информации. Сформулированы предпосылки для конкретизации направлений исследования DLP-систем в целях предотвращения утечек информации в корпоративных, автоматизированных системах различного назначения.

Ключевые слова: DLP-система, канал утечки информации, информационная безопасность, BYOD-технология, симплексный метод.

A.S. Shaburov, **E.E. Zhurilova**

Perm National Research Polytechnic University, Perm, Russian Federation

MODEL OF IDENTIFICATION OF INFORMATION LEAKS CHANNELS IN AUTOMATED SYSTEMS BASED ON THE SYMPLEX METHOD

The article considers trends in modern technologies for processing and transmitting information, as well as the current threats to information security caused by this. There are presented specifics of the implementation of computer attacks on corporate networks, there are grounded features of business processes of information processing that generate information leakage channels. Also there are determined the most effective ways to prevent information leakage, through the control of data flows, using DLP-systems and technologies. There are given the information of practical experience of counteraction to information leakage channels, which allowed to formulate the basic principles of combating this phenomenon, and also to formulate basic groups of criteria for evaluating their effectiveness. At the same time, the one of the main factors for choosing a DLP solution is the quantitative detection of information leakage channels. This article gives the statistics of distribution of probabilities of realizations of the most actual threats of information security for the last period. Conclusions are made about the characteristic changes in statistical data. It gives a brief description of the simplex method used as the basis for constructing the model representation. The problem of constructing a mathematical model is formulated. Based on statistical data, using a simplex method, has been developed a mathematical model that describes the change in the probability of the implementation of information leaks through various channels. At the same time, the growth trends in the volume of information resources of corporate systems are taken into account. Based on the received data, two most relevant leakage channels were identified for the period under study, and projections of the situation development were given. In this article was determined the possibility of DLP-systems for monitoring information leakage channels. The prerequisites are formulated for concretizing the research directions of DLP-systems, in order to prevent information leaks in corporate, automated systems for various purposes.

Keywords: DLP-system, information leakage channels, information security, BYOD-technology, simplex method.

Развитие современных технологий обработки и передачи информации способствует появлению новых угроз безопасности информации. Это связано с возможностью утраты конфиденциальности, целостности информации, искажения, раскрытия данных, адресованных или принадлежащих конечным пользователям. Подобная тенденция характерна для различных сфер хозяйственной и профессиональной деятельности. Особенно подобные явления чреваты последствиями для корпоративных систем финансового сектора, банковской сферы, где свыше 90 % всех преступлений обусловлены внедрением автоматизированных систем обработки информации.

В условиях снижения возможности контроля сетевого периметра корпоративная инфраструктура в последнее время перестала быть главной целью кибератак, а профиль угроз сместился в сторону Data-

центричности, когда внешние атаки направлены на завладение корпоративными данными [1].

При этом современные компьютерные атаки на данные чаще всего реализуются на уровнях выше сетевого через уязвимости прикладного программного обеспечения либо под влиянием человеческого фактора, выражающегося в слабой дисциплине и низкой компьютерной грамотности пользователей.

В то же время значимость выполнения требований политики информационной безопасности при использовании корпоративных данных в последнее время возрастает. Это связано, прежде всего, с процессом внедрения в корпоративный сектор технологий и сервисов широкого потребления для обеспечения решения бизнес-процессов различного назначения. Бизнес-процессы предполагают использование корпоративных рабочих станций, мобильных и портативных устройств, функционирующих по технологии «тонкий клиент». Зачастую могут применяться домашние компьютеры, а также внедряться BYOD-технология. Использование подобных технологических приемов позволяет полноценно создавать, обрабатывать, хранить и передавать корпоративные данные.

В то же время пользователь при использовании различных устройств и сетевых сервисов становится центральным звеном в информационных процессах и источником распространения данных. При этом периметры корпоративной сети зачастую становятся прозрачными для внешних воздействий, что снижает возможность контроля и блокировки утечек информации традиционными средствами защиты.

В практике защиты корпоративной сети основой является именно предотвращение утечек, построенное по принципу минимальных привилегий: вводится запрет использования ряда сервисов и устройств пользователями, которым эти сервисы и устройства по работе не нужны. При необходимости использования тех или иных сервисов доступ предоставляется, и ведется активный мониторинг использования как самих устройств, так и сервиса.

Зачастую решение подобной проблемы связано со сложностью выявления подобных каналов, их идентификации и принятия оперативного решения по их блокированию. Опыт противодействия каналам утечек информации позволил сформировать базовые принципы борьбы с данным явлением, основанном на разработке и внедрении

комплексной системы защиты информации. Внедрение комплексных систем защиты зачастую связано с наиболее эффективным способом предотвращения утечки информации посредством контроля потоков данных с использованием DLP-систем и технологий [2].

Ключевым показателем эффективности для полнофункциональной DLP-системы должно быть качество решения проблемы утечки данных. Это означает, что система должна, в первую очередь, обеспечивать нейтрализацию наиболее опасных векторов угроз утечки информации. При этом негативное влияние угроз должно быть снижено в дополнение к нейтрализации ключевых угроз посредством мониторинга и контроля всех основных каналов утечки информации во всех сценариях, связанных с этим вектором угроз.

Одним из основных факторов для выбора DLP-решения является фактор количественного выявления каналов утечки информации. Кроме того, выбор может осуществляться как с учетом нормативно-правовых аспектов внедрения DLP-системы [3], так и с учетом особенностей применяемого для выявления угрозы алгоритмов морфологического анализа [4] и ряда других параметров.

В то же время опыт внедрения, эксплуатации и оценки подобных систем позволил сформировать основные, базовые группы критериев оценки эффективности. Так, по информации от независимой исследовательской компании Forrester Research выделяются четыре критерия оценки эффективности DLP-систем [5]:

- многоканальность;
- унифицированный менеджмент;
- активная защита;
- классификация информации с учетом как ее содержимого, так и контекста самой информации.

Быстродействие DLP-системы зависит от объемов обрабатываемой информации и корректности составленных правил обработки информации. Чем корректнее составлены правила, тем меньше ошибок и ложных срабатываний и тем меньше количество времени, требуемое для выяснения истины.

Разработка системы защиты информации от утечки по различным каналам зачастую сопряжена с проблемой наличия слишком большого количества этих каналов для реализации системы защиты, стоимость которой бы не превышала стоимости ущерба от реализации утечек по этим каналам.

Возможным решением данной проблемы является нахождение среди множества каналов нескольких наиболее актуальных, защита которых часто реализуется в информационных системах рассматриваемого типа.

Существует несколько методов ранжирования, включая экспертный опрос, экспертную оценку, методы математического моделирования и различные статистические методы с элементами теории вероятностей.

Исследования DLP-систем на перекрытие каналов утечек информации не являются исключением. Хотя такие системы предотвращают утечку информации по большинству каналов, невозможно провести исследование всех каналов одновременно и получить достоверные результаты при соизмеримых затратах.

Выбор нескольких наиболее актуальных каналов утечки информации, которые перекрывают DLP-системы, предполагается на основе построения математической модели утечки по выборке данных нескольких лет наблюдений с использованием симплексного метода математического моделирования нелинейных систем. В качестве исходных данных предполагается использовать статистику утечек информации по различным каналам за период 2009–2016 гг. (таблица).

Статистика утечек информации по различным каналам в 2009–2016 гг.

Каналы утечек	Годы							
	2009	2010	2011	2012	2013	2014	2015	2016
Сеть	18,2	16	13,6	6,7	13,8	35,1	45,6	69,5
Электронная почта	5,3	7	6,2	6,3	10,9	8,2	7,5	8,5
Бумажные документы	19,9	20	19,1	22,3	21,9	17,7	14	10,8
IM (текст, голос, видео)	7,2	5	6,6	3	4,1	1	0,2	2
Утрата оборудования	14,6	25	13,9	15	17,3	15,9	7,6	4,8
Мобильные устройства	13,3	12	9,6	9,6	1,5	0,6	0,3	0,4
Съемные носители	4,6	8	6,2	6	5	3,6	3,6	4,1
Не определено	16,9	7	24,8	31,1	25,5	17,9	21,3	0

Очевидно из приведенных данных таблицы, начиная с 2009 г., утечки бумажных документов уменьшились на 9,1 % в отличие от утечек через сеть, которые выросли почти в 4 раза.

Интенсивность утечек по другим каналам менялась разнонаправленно в различные периоды, поэтому для качественного выбора каналов утечек для исследования построим математическую модель на основе симплексного метода.

Симплекс – это простейший выпуклый многогранник, образованный n+1 вершинами в n-мерном пространстве, которые соединены между собой прямыми линиями [6].

Суть симплексного метода заключается в последовательном отражении вершины симплекса с наибольшими функциями ошибок, что постепенно приводит к стяжению симплекса в точку, координаты которой будут искомыми параметрами [7, 8].

В качестве искомых параметров выберем соответствующие коэффициенты при использовании следующих характеристиках каналов утечки информации:

1) особенности сети;
2) электронная почта;
3) IM (текст, голос, видео);
4) мобильные устройства;
5) съемные носители.

Однако для построения более точной модели целесообразно учитывать все перечисленные выше характеристики. Остальные параметры таблицы будут исключены из рассмотрения коэффициентов готовой модели в связи с тем, что контролировать утечки по этим каналам DLP-системы не способны.

Задача состоит в том, чтобы построить такую модель, которая бы точно описывала изменение объема утечек по различным каналам [9, 10, 12, 13].

Уравнение модели имеет следующий вид:

$$y = b_1 x_1 + b_2 x_2^3 + b_3 x_3^4 + b_4 Ln(x_4) - b_5 x^2 + b_6 x_6 + b_7 x_7^5 - b_8 \sqrt{x_8}. \qquad (1)$$

Зададим коэффициент отражения $\gamma_o = 1$, коэффициент растяжения $\gamma_r = 2$ и коэффициент сжатия $\gamma_s = 0{,}5$, опираясь на которые будут строиться новые симплексы.

Также зададим два условия окончания счета:

1. Значение функции ошибок должно быть не более 10^{-3}.

$$\sqrt{\frac{\sum_i (F_i - \overline{F})^2}{m}} \le 10^{-3}. \qquad (2)$$

2. Максимальная погрешность не должна превышать 10^{-3}.

Алгоритм работы программы представлен на рис. 1.

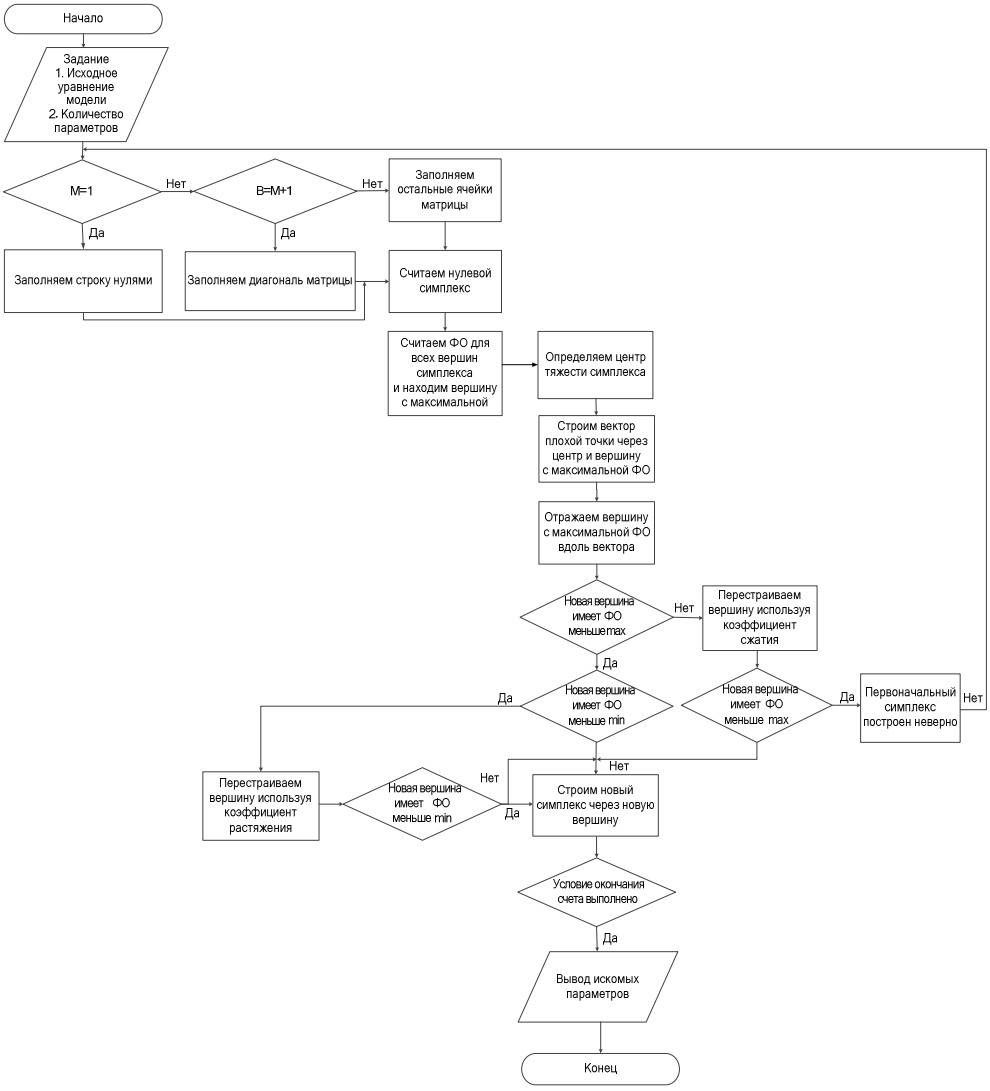

Рис. 1. Алгоритм работы программы

На начальном этапе необходимо рассчитать и построить исходный симплекс по исходным данным, после чего происходит построение нового симплекса. Для этого находится вершина в имеющемся симплексе с максимальной функцией ошибок, после этого она отражается вдоль вектора, построенного через старую вершину и центр тяжести симплекса. При необходимости применяются процедуры сжатия или растяжения, чтобы уменьшить значение функции ошибок для новой вершины.

Новый симплекс строится уже через новую точку, в котором находится вершина с максимальной функцией ошибок, и последовательность действий повторяется заново.

Алгоритм работы программы продолжается до тех пор, пока не будет найдено оптимальное значение, т.е. пока симплекс не сведется к точке, идеальному решению. Результатом работы алгоритма должны стать коэффициенты, подобранные для заданного уравнения, на основании которого строился исходный симплекс. Подпор коэффициентов осуществляется таким образом, чтобы выходные параметры модели совпадали с заданными с учетом погрешности.

В реальных вычислениях идеальное решение подобрать практически невозможно, поэтому для окончания работы алгоритма поставлены два других условия – максимальная погрешность и максимальное значение функции ошибок, указанные выше [5]. По итогам работы программы были получены следующие значения коэффициентов модели:

$$b_1 = 1{,}5191;\ b_2 = 0{,}0106;\ b_3 = -0{,}0027;\ b_4 = -0{,}5806;$$
$$b_5 = -0{,}0143;\ b_6 = -1{,}57;\ b_7 = 0{,}00003;\ b_8 = -0{,}3971.$$

Уравнение модели, соответствующей исходным данным, имеет вид:

$$y = 1{,}5191x_1 + 0{,}0106x_2^3 - 0{,}0027x_3^4 - 0{,}5806Ln(x_4) - \\ -0{,}0143x_5^2 - 1{,}57x_6 - 0{,}003x_7^5 - 0{,}3971\sqrt{x_8}. \quad (3)$$

На рис. 2 представлены выходные параметры модели, заданные и полученные на этом этапе. Анализ данных параметров, с учетом заданной погрешности результатов, позволяет сделать вывод об их адекватности исследуемым процессам.

Как указано выше, в данной модели вводятся ограничения на учет следующих каналов: «Бумажные документы», «Утрата оборудования» и «Неизвестные каналы». Учет данных каналов при анализе коэффициентов не считается целесообразным, поскольку DLP-системы не имеют функционала для перекрытия таких каналов [11, 14].

Отрицательные коэффициенты указывают на снижение актуальности каналов утечки, что также видно и по таблице, например для параметра 4.

Очевидно, что наибольшие коэффициенты при характеристиках 1, 2 и 7, т.е. «Сеть», «Электронная почта» и «Съемные носители». Это означает, что объем утечек по данным характеристикам увеличивается,

а следовательно, при выявлении каналов утечек информации, которые может блокировать DLP-система, в первую очередь рационально исследовать их.

```
Lambda[1] = 1.519069492
Lambda[2] = 0.010622852
Lambda[3] = -0.002683299
Lambda[4] = -0.580615601
Lambda[5] = -0.014311107
Lambda[6] = -1.570004701
Lambda[7] = 0.000269981
Lambda[8] = -0.397064567

 Измеренные значения     Модель
       100.0000            92.4559
       100.0000           101.9125
       100.0000            81.7612
       100.0000           115.5774
       100.0000            98.6206
       100.0000           104.6129
       100.0000            93.2144
       100.0000           104.5621
```

Рис. 2. Результат работы программы

По результатам исследования сформировался следующий перечень каналов утечки информации для их дальнейшего анализа и рассмотрения в рамках выбора оптимального DLP-решения:

1) сетевые каналы, в том числе различные мессенджеры, социальные сети, торренты и прочее;

2) электронная почта;

3) съемные носители, за исключение мобильных устройств.

Таким образом, проведя анализ статистических данных утечек информации и на основании построенной с помощью симплекс-метода математической модели, можно сделать вывод о росте объема и актуальности утечек через сетевые каналы связи. Следовательно, при оценке рынка DLP-систем и их влияния на бизнес-процессы организации, а также при возможности внедрения их в корпоративные сети необходимо уделять особое внимание данным каналам утечки информации. Это, в свою очередь, позволит выбирать решения, которые смогут наиболее качественно осуществить защиту от данного вида угроз информационной безопасности.

Библиографический список

1. Принципы полноценного DLP-контроля [Электронный ресурс] // Информационная безопасность. – 2017. – № 3. – URL: http://search.groteck.ru:17000/hl?url=http%3A//www.itsec.ru/articles2/dlp/printsipy-polnotsennogo-dlp-kontrolya&mime=text/html&charset=windows-1251&hldoclist=http%3A//search.groteck.ru%3A17000/%3Ftext%3D%25E1%25EE%25F0%25FC%25E1%25E0%2B%25F1%2B%25F3%25F2%25E5%25F7%25EA%25E0%25EC%25E8%2B2017 (дата обращения: 20.09.2017).

2. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP-системы на основе Falcongaze Secure Tower // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2015. – № 4(16). – С. 57–67.

3. Шабуров А.С., Журилова Е.Е. О нормативно-правовых аспектах внедрения DLP-систем // Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2015. – № 3(17). – С. 37–41.

4. Шабуров А.С., Журилова Е.Е. Особенности реализации алгоритмов морфологического анализа в DLP-системах // Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2016. – № 2(20). – С. 23–28.

5. Персональный сайт группы компаний Infowatch [Электронный ресурс] // Infowatch.ru. – 2003. – URL: https://www.infowatch.ru/analytics/reports (дата обращения: 20.09.2017).

6. Основы теории и техники физического моделирования и эксперимента: учеб. пособие / Н.Ц. Гатапова, А.Н. Колиух, Н.В. Орлова, А.Ю. Орлов. – Тамбов, 2014. – 77 с.

7. Леготкина Т.С. Моделирование систем управления. Исследование нелинейных моделей: учеб.-метод. пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 2004.

8. Леготкина Т.С., Данилова С.А. Моделирование систем управления: учеб. пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 2008.

9. Кубланов М.С. Математическое моделирование. Методология и методы разработки математических моделей механических систем и процессов: учеб. пособие. Ч. I: Моделирование систем и процессов. – 3-е изд., перераб. и доп. – М.: Изд-во МГТУ ГА, 2004. – 108 с.

10. Шорохова И.С., Кисляк Н.В., Мариев О.С. Статистические методы анализа: учеб. пособие. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 300 с.

11. Сердюк В., Ванерке Р. DLP на страже информации [Электронный ресурс] // Информационная безопасность. – 2017. – Вып. 3. – URL: http://www.itsec.ru/articles2/dlp/dlp-na-strazhe-informatsii (дата обращения: 25.07.2017).

12. Банди Б. Основы линейного программирования: пер. с англ. – М.: Радио и связь, 1989. – 176 с.

13. Шевченко В.Н., Золотых Н.Ю. Линейное и целочисленное линейное программирование. – Н. Новгород: Изд-во Нижегород. гос. ун-та им. Н.И. Лобачевского, 2004. – 154 с.

14. Ковалев А. Функционал DLP: самое главное в системах защиты от утечек [Электронный ресурс] // Информационная безопасность. – 2012. – Вып. 4. – URL: http://www.itsec.ru/articles2/Oborandteh/funktsional-dlp-samoe-glavnoe-v-sistemah-zaschity-ot-utechek/ (дата обращения: 22.07.2017).

References

1. Printsipy polnotsennogo DLP-kontrolia [Principles of high-grade DLP-control]. *Informatsionnaia bezopasnost'*, 2017, no. 3, available at: http://search.groteck.ru:17000/hl?url=http%3A//www.itsec.ru/articles2/dlp/printsipy-polnotsennogo-dlp-kontrolya&mime=text/html&charset=windows-1251&hldoclist=http%3A//search.groteck.ru%3A17000/%3Ftext%3D%25E1%25EE%25F0%25FC%25E1%25E0%2B%25F1%2B%25F3%25F2%25E5%25F7%25EA%25E0%25EC%25E8%2B2017 (accessed 20 September 2017).

2. Shaburov A.S., Zhurilova E.E., Luzhnov V.S. Tekhnicheskie aspekty vnedreniia DLP-sistemy na osnove Falcongaze Secure Tower [Technical aspects of implementation of DLP-systems, based on Falcongaze Secure Tower]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2015, no. 4(16), pp. 57-67.

3. Shaburov A.S., Zhurilova E.E. O normativno-pravovykh aspektakh vnedreniia DLP-sistem [On the regulatory and legal aspects of implementing DLP-systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk, 2015, no. 3(17), pp. 37-41.

4. Shaburov A.S., Zhurilova E.E. Osobennosti realizatsii algoritmov morfologicheskogo analiza v DLP-sistemakh [Features of the implementation of algorithms for morphological analysis in DLP-systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk, 2016, no. 2(20), pp. 23-28.

5. Personal'nyi sait gruppy kompanii Infowatch [Personal site of the group of companies Infowatch]. Infowatch.ru, 2003, available at: https://www.infowatch.ru/analytics/reports (accessed 20 September 2017).

6. Gatapova N.Ts., Koliukh A.N., Orlova N.V., Orlov A.Iu. Osnovy teorii i tekhniki fizicheskogo modelirovaniia i eksperimenta [Fundamentals of the theory and technique of physical modeling and experiment]. Tambov, 2014. 77 p.

7. Legotkina T.S. Modelirovanie sistem upravleniia. Issledovanie nelineinykh modelei [Modeling of control systems. Study of nonlinear models]. Permskii gosudarstvennyi tekhnicheskii universitet, 2004.

8. Legotkina T.S., Danilova S.A. Modelirovanie sistem upravleniia [Modeling of control systems]. Permskii gosudarstvennyi tekhnicheskii universitet, 2008.

9. Kublanov M.S. Matematicheskoe modelirovanie. Metodologiia i metody razrabotki matematicheskikh modelei mekhanicheskikh sistem i protsessov. Chast' I: Modelirovanie sistem i protsessov [Math modeling. Methodology and methods for developing mathematical models of mechanical systems and processes. Part I. Modeling systems and processes]. 3nd ed. Moskovskii gosudarstvennyi tekhnicheskii universitet grazhdanskoi aviatsii, 2004. 108 p.

10. Shorokhova I.S., Kisliak N.V., Mariev O.S. Statisticheskie metody analiza [Statistical methods of analysis]. Ekaterinburg: Ural'skii universitet, 2015. 300 p.

11. Serdiuk V., Vanerke R. DLP na strazhe informatsii [DLP on guard of information]. *Informatsionnaia bezopasnost'*, 2017, iss. 3, available at: http://www.itsec.ru/articles2/dlp/dlp-na-strazhe-informatsii (accessed 25 July 2017).

12. Bandi B. Osnovy lineinogo programmirovaniia [Fundamentals of linear programming]. Moscow: Radio i sviaz', 1989. 176 p.

13. Shevchenko V.N., Zolotykh N.Iu. Lineinoe i tselochislennoe lineinoe programmirovanie [Linear and integral linear programming]. Nizhegorodskii gosudarstvennyi universitet imeni N.I. Lobachevskogo, 2004. 154 p.

14. Kovalev A. Funktsional DLP: samoe glavnoe v sistemakh zashchity ot utechek [DLP Functionality: The Most Important in Leakage Protection Systems]. *Informatsionnaia bezopasnost'*, 2012, iss. 4, available at: http://www.itsec.ru/articles2/Oborandteh/funktsional-dlp-samoe-glavnoe-v-sistemah-zaschity-ot-utechek/ (accessed 22 July 2017).

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Журилова Елена Евгеньевна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: ele11485995@yandex.ru).

About the authors

Shaburov Andrey Sergeevich (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor at the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Zhurilova Elena Evgen'evna (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: ele11485995@yandex.ru).

Получено 09.10.2017