ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ ПРИ СРАВНЕНИИ DLP-СИСТЕМ

Зверев Илья Николаевич
аспирант кафедры информационных технологий Ульяновского Государственного Университета, РФ, г. Ульяновск
E-mail: inz_2008@mail.ru

APPLICATION OF HIERARCHY ANALYSIS METHOD COMPARISON DLP-SYSTEMS

Ilya Zverev
post-graduate student at the Department of Information Technologies at Ulyanovsk State University, Russia, Ulyanovsk

АННОТАЦИЯ

Целью настоящей статьи является определение критериев и методологии сравнения систем защиты информации от утечек (DLP-систем). В качестве метода предлагается использование метода анализа иерархий. Предлагаются критерии сравнения и вид иерархии на примере сравнения трех DLP-систем отечественной разработки. Полученные результаты могут служить в дальнейшем основой для анализа существующих DLP-систем.

ABSTRACT

The purpose of this article is to define the criteria and methodology comparison sys-tems to protect information from leaks (DLP-systems). As a method is proposed the use of the method of analysis of hierarchies. Proposed criteria for comparison and view hierarchy in the example of comparison of the three systems DLP-home development. The results obtained can serve as a basis for further analysis of existing DLP-systems.

Ключевые слова: защита информации; DLP; защита информации от утечек; метод анализа иерархий.

Keywords: information protection; DLP; data leak prevention; analytic hierarchy process.

В последние годы осложнилась ситуация с внутренними угрозами, в частности с инсайдерами (злоумышленниками, являющихся членами организации-владельца конфиденциальной информации). В связи с этим, для защиты информации от утечек было создано новое направление в области информационной безопасности — так называемые DLP-системы.

В литературе по информационной безопасности [1] дается следующее определение:

DLP-системы (Data Leak Prevention) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Сравнение и выбор DLP-систем для защиты информации в конкретной автоматизированной системе — непростая задача. Руководителям, принимающим решение о закупке и внедрении данных систем, приходится разбираться в новой для себя предметной области, не имея независимой информации о характеристиках. Кроме того, на сегодняшний день не выработано четких критериев и методологии сравнения DLP-систем.

Предметом исследования настоящей статьи является решение данной проблемы, т. е. определение критериев и предложение метода сравнения (оценки) DLP-систем.

Исходя из определения DLP-систем очевидно, что ключевой характеристикой системы должна являться возможность контролировать различные каналы утечки информации и анализировать потоки информации, проходящие по этим каналам.

Поэтому основные критерии должны определяться:

1. контролем различных каналов утечки информации;

2. использованием методов защиты информации от утечек (методов анализа информации на предмет наличия защищаемой информации).

В качестве дополнительного критерия будет определяться наличие действующего сертификата по требованиям безопасности на DLP-систему.

1. Основные каналы утечки информации

Для определения критериев сравнения DLP-систем необходимо сначала определить основные угрозы (каналы) утечки информации.

Выделим основные категории каналов утечки с позиций DLP-системы. DLP-системы могут контролировать:

- печать документов. Далее по тексту — канал 1;
- подключение внешних устройств. Далее по тексту — канал 2;
- передачу информации через Internet. Далее по тексту — канал 3;

2. Методы защиты информации от утечек

В таблице 1 приведены основные методы (технологии) защиты информации от утечек и их краткое описание.

Таблица 1.

Методы защиты информации от утечек

Метод (группа методов)	**Краткое описание**
Поиск по регулярным выражениям (метод 1)	С помощью некоторого языка регулярных выражений определяется «маска», структура данных, которые относятся к конфиденциальным. В качестве примера можно привести номера кредитных карт, паспортные данные и т. д.
Лингвистический анализ (словоформы, синонимы, морфология и т. п.) (метод 2)	Этот подход называют еще контекстным и морфологическим. Определение конфиденциальной информации производится на основе выделения в ней множества значимых, определяющих содержание слов, называемых также ключевыми.
Анализ транслита (метод 3)	Поиск замаскированного с помощью транслитерации текста.
Анализ замаскированного текста (метод 4)	Поиск замаскированного текста. Для анализа используются статистические методы, а также методы поиска информации в определенных областях (файлов).

Анализ с использованием цифровых отпечатков (метод 5)	Этот метод основан на построении некоторого идентификатора исходного текста. Реализуется следующий автоматический алгоритм: 1) Из документа выделяется текстовое содержание. 2) Текст некоторым образом разбивается на фрагменты. 3) Для каждого такого фрагмента система создает некий идентификатор («отпечаток».) 4) Конфиденциальный документ представляется в системе набором таких «отпечатков». Для сопоставления проверяемого текста с множеством конфиденциальных документов для него «на лету» строится аналогичный набор «отпечатков». Если оба множества отпечатков демонстрируют, система диагностирует попытку утечки.
Гибридный анализ (метод 6)	Интегрирование лингвистического, статистического и других методов в единый алгоритм анализа информации, контроля и детектирования.

3. Методология сравнения

В качестве метода сравнения DLP-систем предлагается использовать метод анализа иерархий [2].

Метод анализа иерархий (МАИ) — математический инструмент системного подхода к сложным проблемам принятия решений. МАИ не предписывает лицу, принимающему решение (ЛПР), какого-либо «правильного» решения, а позволяет ему в интерактивном режиме найти такой вариант (альтернативу), который наилучшим образом согласуется с его пониманием сути проблемы и требованиями к ее решению. Этот метод разработан американским математиком Томасом Саати.

Порядок применения метода анализа иерархий:

1) Определение цели, альтернативных вариантов достижения цели.

2) Построение качественной модели проблемы в виде иерархии с определением критериев для оценки качества альтернатив.

3) Определение приоритетов всех элементов иерархии с использованием метода парных сравнений.

4) Синтез глобальных приоритетов альтернатив путем линейной свертки приоритетов элементов на иерархии.

5) Проверка суждений на согласованность.

6) Принятие решения на основе полученных результатов.

4. Определение цели и выбор альтернатив

Целью будет являться **успешный выбор одной из DLP-систем**, предназначенной для защиты информации от утечек в корпоративной автоматизированной системе.

В качестве альтернатив будут взяты 3 наиболее популярные российские DLP-системы:

- Дозор-Джет 4.0 (Инфосистемы Джет) — далее по тексту DLP-система **A**;
- InfoWatch Traffic Monitor Enterprise 3.5 (InfoWatch) — далее по тексту DLP-система **B**;
- ЫусгкШЕ Япфеу 3ю0 и ЫусгкШЕ Ядщсл 3ю0 (ЫусгкШЕ) — далее по тексту ВДЗ-система **С**ю

5. Построение иерархии

На рисунке 1 представлена модель проблемы (иерархия), содержащая цель, альтернативы и критерии оценки.

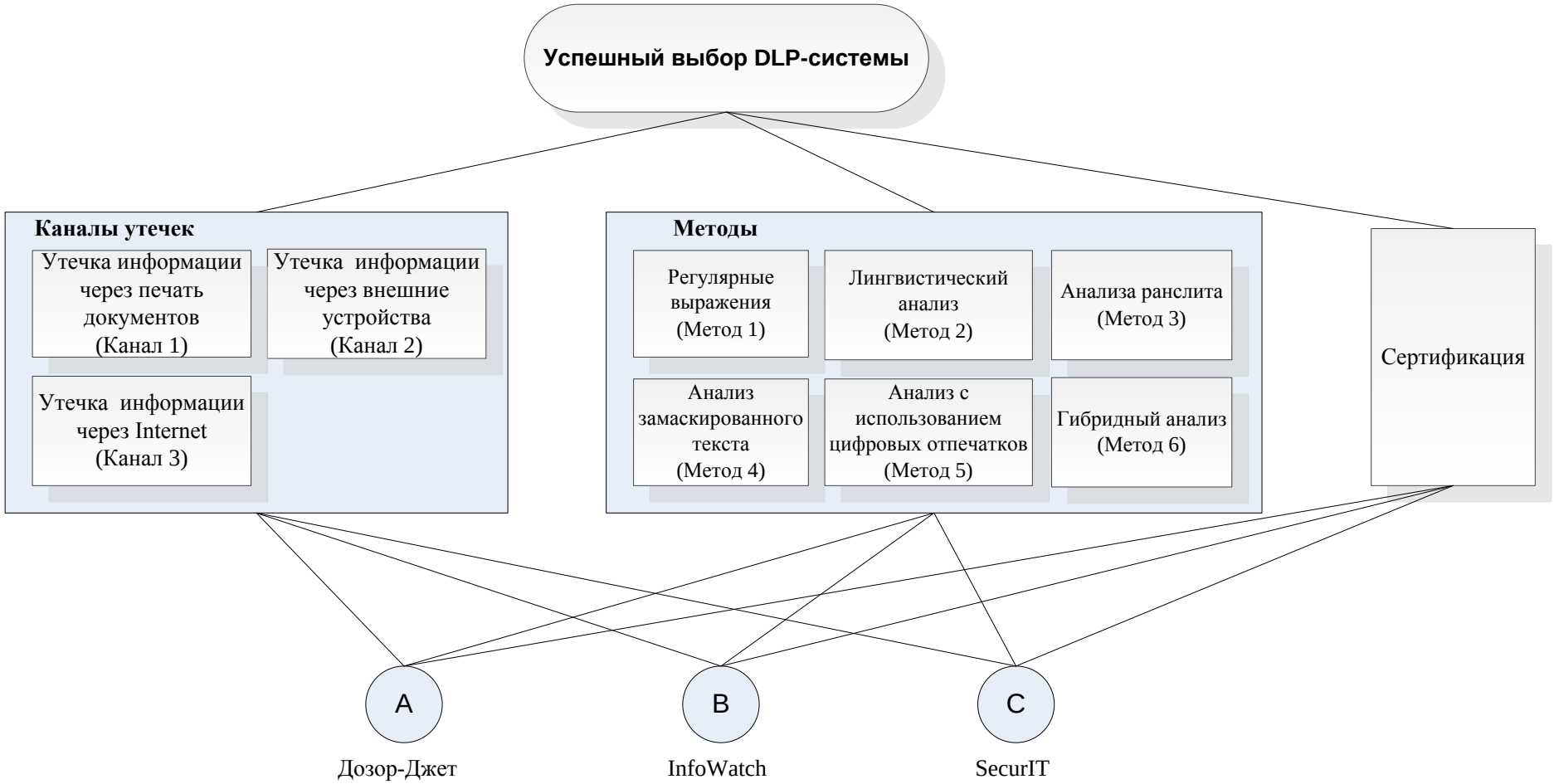

Рисунок 1. Иерархия проблемы

Итак, для достижения цели выбор производится из 3-х DLP-систем по 10 независимым характеристикам (3 канала утечек + 6 методов защиты + сертификация).

Для проведения сравнения эксперту необходимо получить информацию (исходные данные) о том, какие каналы утечки закрываются сравниваемыми DLP-системами и какие методы они при этом используют.

Данные для настоящего сравнения получены с сайтов производителей, из документации и по результатам тестирования ознакомительных версий программ.

6. Определение приоритетов

Для определения приоритетов составляются матрицы попарных сравнений (таблица 2). В роли эксперта выступал автор настоящей статьи, основываясь на выше изложенной информации (характеристиках сравниваемых DLP-систем и представлениях об объекте защиты). Сравнения проводились по шкале значимости от 1 до 9 (1 — одинаковая значимость, 3 — незначительное превосходство и т. д., обратные величины — если сравниваемый объект уступает в данной характеристике).

В реальной жизни экспертами могут выступать специалисты по защите информации, руководители предприятия. Главное требование — эксперты в совокупности должны знать специфику защищаемой автоматизируемой системы и иметь квалифицированные знания в области защиты информации от утечек.

Таблица 2.

Матрица попарных сравнений

	Канал 1	**Канал 2**	**Канал 3**	**Метод 1**	**Метод 2**	**Метод 3**	**Метод 4**	**Метод 5**	**Метод 6**	**Серт.**
Канал 1	1	1/3	1/5	1	1	1	1	1	1	1/3
Канал 2	3	1	1/3	1	1	1	1	1	1	1/3
Канал 3	5	3	1	1	1	1	1	1	1	1/3
Метод	1	1	1	1	1/9	1/7	1/7	1/7	1/7	1/3

1										
Метод 2	1	1	1	9	1	5	3	1	3	1/3
Метод 3	1	1	1	7	1/5	1	1	1/5	1/7	1/3
Метод 4	1	1	1	7	1/3	1	1	1/5	1/7	1/3
Метод 5	1	1	1	7	1	5	5	1	1/3	1/3
Метод 6	1	1	1	7	1/3	7	7	3	1	1/3
Серт.	3	3	3	3	3	3	3	3	3	1

Для каждой из матриц N_i определяется нормализованный вектор локальных приоритетов, со следующими компонентами:

$$\sqrt[n]{\prod_{l=1}^{n} a_{jl}} = a_j$$

где n размерность матрицы — a_{ji} элемент -j-ой строки матрицы. Таким образом, матрице N_i сопоставляется вектор a_i.

Нормирование компонент осуществляется путем деления каждой компоненты вектора $\boldsymbol{a_i}$ на сумму всех компонент этого вектора:

$$b_j = \frac{a_j}{\sum_j a_j}$$

Далее считаются приоритеты для сравнения альтернатив по всем критериям (таблица 3).

Таблица 3.

Приоритеты сравнения альтернатив по всем критериям

	Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6	Серти-Фика-ция
A	0,08	0,33	0,26	0,33	0,14	0,08	0,08	0,33	0,09	0,08

B	0,46	0,33	0,1	0,33	0,72	0,46	0,46	0,33	0,45	0,18
C	0,46	0,33	0,64	0,33	0,14	0,46	0,46	0,33	0,45	0,73

Полученный вектор приоритетов для сравнения значимости критериев между собой приведен в таблице 4.

Таблица 4.

Приоритеты значимости критериев

Канал 1	Канал 2	Канал 3	Метод 1	Метод 2	Метод 3	Метод 4	Метод 5	Метод 6	Серти-фикация
0,059	0,077	0,1	0,02	0,13	0,057	0,059	0,116	0,139	0,23

Перемножив одну матрицу на другую, получаем итоговый вектор приоритетов для альтернатив (A — 0,17; B — 0,36; C — 0,46).

7. Проверка суждений на согласованность

После получения данных (обработки матриц) следует определить их согласованность. Степень согласованности для каждой матрицы приближенно вычисляется следующим способом: суммируется каждый столбец матрицы суждений, и сумма первого столбца умножается на величину первой компоненты нормализованного вектора приоритетов и т. д., затем полученные значения суммируются [2]:

$$\lambda_{max} = \sum_{i=1}^{n} \left(b_j \sum_{j=1}^{n} a_{ji} \right)$$

Далее вычисляется индекс согласованности:

$$ИС = (\lambda_{max} - n)/(n-1)$$

Отношение ИС к среднему случайному индексу ($СИ_{ср}$) согласованности для матрицы того же порядка называется отношением согласованности (ОС).

$$ОС = ИС/СИ_{ср}.$$

Зачения $СИ_{ср}$ для используемых матриц порядка 3 и 10 равно 0,58 и 1,49 соответственно [2].

Значение ОС, входящее в интервал от 0 до 0,1 будем считать приемлемым.

Проведем описанные выше вычисления и получаем для 11 матриц сравнения следующие значения, приведенные в таблице 5.

Таблица 5.

Матрица согласованности суждений

λ_{max}	12	3,16	3	3	3,005	3	3,16	3,16	3	3	3
ИС	0,22	0,08	0	0	0,002 5	0	0,08	0,08	0	0	0
ОС	0,14	0,12	0	0	0,004	0	0,12	0,12	0	0	0

Большая часть матриц имеют согласованные суждения (7 из 11), для остальных отклонение от нормы несущественно. Таким образом, можно сделать вывод в целом о согласованности суждений эксперта, проводившего сравнение.

8. Принятие решения на основе полученных результатов

По результатам проведенных вычислений получаем значения общего ранжирования альтернатив:

$$A = 0,17;\ B = 0,36;\ C = 0,46.$$

Таким образом, наиболее приемлемой альтернативой для оценивающего эксперта является DLP-система SecurIT Zgate компании Zecurion.

Заключение

В данной статье определены критерии и предложена методология сравнения DLP-систем. С помощью предложенного метода проведен сравнительный анализ систем российских разработчиков.

Методология и критерии сравнения DLP-систем, предложенные в настоящей статье, позволят более грамотно подойти к процессу выбора

системы защиты информации от утечек для защищаемой автоматизированной системы.

Список литературы:

1. Глобальное исследование утечек информации за 2013 год [Электронный ресурс] — Режим доступа. — URL: https://www.infowatch.ru/report2013 (дата обращения: 01.04.2014).
2. Томас Саати. Принятие решений. Метод анализа иерархий. М., «Радио и связь», 1993 г — 278 с.