УДК 004.056.53 + 658.1 : 004.056.53 Вестник УрФО № 4(22) / 2016, с. 15–20

Шабуров А. С., Журилова Е. Е.

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ DLP-РЕШЕНИЙ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ СИСТЕМ

В данной статье проанализированыварианты оценки эффективности DLP-систем, с учетом различных факторов их применения для защиты корпоративных систем. Представлена классификация критериев эффективности применения DLP-систем. Разработана математическая модель выбора эффективного DLP-решения, с учетом коэффициента защищенности и выявления утечки информации в ходе бизнес- процессов. Приведена структурная модель оценки эффективности DLP-систем, с учетом минимально допустимых параметров обнаружения утечек информации по различным каналам.

Ключевые слова: *DLP-система, бизнес-процесс, активная защита, оценка эффективности*

Shaburov A. S., Zhurilova E. E.

MODEL ASSESSING THE EFFECTIVENESS OF APPLICATION DLP-SOLUTIONS TO PROTECT CORPORATE SYSTEMS

In this article analyzes the options for assessing the effectiveness of DLP-systems, taking into account of the various factors of their application to protect corporate systems. It show the classification of criteria efficiency of application of DLP-systems. It working out a mathematical model of choice DLP-effective solutions, taking into account the factor of security and detection of information leakage in the course of business - processes.Show the block model evaluation of the effectiveness of DLP-systems, taking into account the minimum permissible parameters of information leakage detection through various channels.

Keywords: *DLP-system,business process, active protection, performance evaluation*

В условиях растущего количества угроз информационной безопасности борьба с утечками информации в корпоративных системах предприятий и организаций остается одной из актуальных задач[1]. Прежде всего, это связано с необходимостью поддержания устойчивости реализации бизнес-процессов, обеспечивающих экономическую и финансовую стабильность хозяйствующих субъектов. В настоящее время рынок средств защиты информации от утечек представляет собой выбор разнообразных решений[2]. Однако, по-

добрать эффективное средство борьбы с утечками информации, подходящее для конкретного предприятия, зачастую является трудной задачей. Это заставляет собственников информационных ресурсов руководствоваться предложениями конкретных разработчиков DLP-систем, зачастую преследующими коммерческую выгоду и не всегда учитывающими особенности функционирования корпоративных систем[3].

Выбор средства противодействия утечкам информации среди DLP-системможет быть основан на различных подходах. Основным фактором 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[4], так и с учетом особенностей применяемого для выявления угрозы алгоритмов морфологического анализа[5] и ряда других параметров. В то же время опыт внедрения, эксплуатации и оценки подобных систем позволили сформировать основные, базовые группы критериев оценки эффективности.

Так, по информации от независимой исследовательской компании Forrester Research, выделяются четыре критерия оценки эффективности DLP-систем[6]:

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

Сущность предлагаемых критериев заключается в следующем. Критерий многоканальности представляет собой требование к DLP-системе охватывать максимально возможное количество каналов утечки информации, начиная от e-mail и заканчивая файловыми операциями.

Следующим критерием является унифицированный менеджмент, представляющий собой наличие единого средства управления всеми компонентами, входящими в состав DLP-системы. В качестве примера реализации этого требования можно назвать возможность управления тремя основными компонентами системы с одной консоли: сервером баз данных, устройством перехвата и агентами на рабочих станциях.

Критерий активной защиты подразумевает наличие возможности реагировать на утечку информации не только пассивно, фиксируя ее факт, но и активно, блокируя канал утечки информации.

Суть четвертого критерия основывается на фиксации не только содержимого документов с конфиденциальной информацией, но и их атрибутов, например, используемого протокола, отправителя, получателя и т.д.

Данный перечень критериев эффективности DLP-системы не является исчерпывающим. Рассмотрим другой их набор, также используемый дляоценки защиты от утечек информации[7]:

- количество ложных срабатываний (ошибки первого рода);

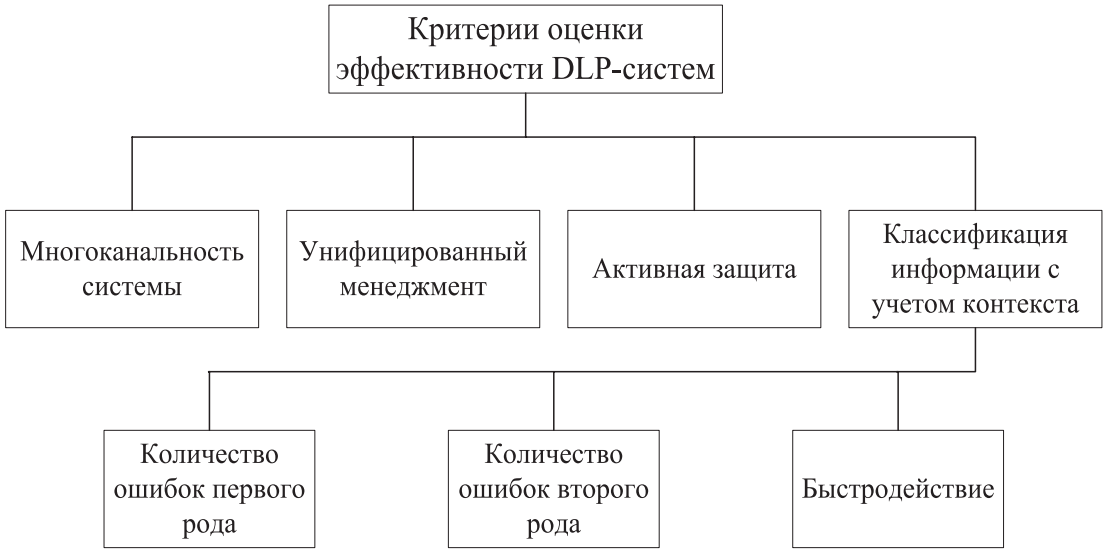

Рис. 1. Критерии оценки эффективности DLP-систем

- количество пропущенных утечек информации (ошибки второго рода);
- быстродействие DLP-системы.

Критерии количества ложных срабатываний и количества пропущенных утечек информации напрямую связаны с качеством морфологического анализа текстов DLP-системамис учетом, как 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.

Представим классификацию критериев оценки эффективности применения DLP-системы в корпоративных сетях, объединив рассмотренные выше классификации, с учетом детализации контекстного анализа (рис. 1).

Сравним четыре наиболее популярных DLP-решения от разных производителей на соответствие приведенным выше критериям эффективности. Поскольку основной функционал DLP-решений сходен, необходимо будет уточнить и расширить приведенные критерии оценки эффективности. В таблице 1 будут рассмотрены только те критерии, оценка которых не требует практического применения моделей.

Возможность мониторинга нескольких каналов передачи данных, как правило, присутствует во всех современных DLP-системах, поэтому в таблице будет оценена так же возможность контроля таких специфических каналов утечки как BitTorrent, QIP, Skype и т.д.

Так же необходимо расширить показатели критерия «Активная защита», обозначив варианты реагирования на инциденты информационной безопасности.

Таблица 1

Сравнение DLP-решений

	Гарда Предприятие	Search Inform	Device Lock DLP	Falcongaze Secure Tower
Многоканальность				
IMAP4S	-	+	-	-
Протоколы авторизации и аутентификации	+	-	-	+
MMP(Mail.ru Агент)	+	+	+	+
XMPP(QIP, Jabber)	+	+	+	+
Skype	+	+	+	+
MS Lync	+	+	+	+
MySpace IM	-	+	-	+
BitTorrent	-	-	-	+
Web траффик в облаке	-	-	-	+
Унифицированный менеджмент				
	+	+	+	+
Активная защита				
Блокировка отправки данных на локальные устройства	+	+	+	+
Запрет доступа к данным для заданных приложений	+	+	-	-
Перемещение конфиденциальных данных в карантин	-	-	+	-
Ограничение доступа в зависимости от типа съемного носителя	+	+	+	+
Блокирование нежелательных процессов	+	+	-	+

Таблица 2

Результаты оценки соответствия критериям эффективности

	Гарда Предприятие	SearchInform	DeviceLockDLP	Falcongaze SecureTower
S%	67%	73%	53%	80%

Проведем оценку соответствия рассматриваемых систем представленным критериям и представим результат в процентном соотношении, результат 100% будет означать максимальное соответствие. Для оценки соответствия воспользуемся следующим соотношением:

$$S_{\%} = \frac{N_{+}}{N} \cdot 100\%,$$

где $S_{\%}$- процент соответствия;

N_{+} - количество положительных результатов по сравнению с критериями;

N – общее количество критериев.

Результаты полученных расчетов представлены в таблице 2.

На основании проведенной оценки выявлено, что наибольшим соответствием по выбранным критериям обладает DLP-система FalcongazeSecureTower, наименее – система DeviceLock.

С другой стороны, DLP-система, обладающая множеством определенных свойствдля реализации основной функции (обеспечить защиту от утечки информации), может отличаться по ряду дополнительных характеристик. К данным характеристикам могут относиться, как рассмотренные ранее в числе критериев эффективности, так и обусловленные свойствами среды применения системы. Условия среды применения системы, в свою очередь, могут способствовать проявлению конкретных угроз безопасности информации, а такжеобусловлены особенностями, протекающих в информационной системе, как отдельных бизнес-операций, так и бизнес-процессов, в целом. Математически это может быть сформулировано в следующем виде:

$$D = \sum_{i=N} K_i m_i, \sum_{i=N} K_i = 1, \qquad (1)$$

где:

D - обобщенный показатель оценки качества DLP - решения (обобщенный коэффициент защищенности, показывающий уровень выявления утечек информации по всей совокупности возможных каналов);

m_i-i-й частный показатель оценки эффективности DLP (частный коэффициент защищенности, показывающий, какой каналутечки i-го вида выявляется);

N-множество частных показателей оценки качества, сводимых в обобщенный показатель;

K_i- весовой коэффициент i-го частного показателя качества в аддитивной свертке.

Коэффициент защищенности (выявления утечки информации) в ходе отдельных бизнес-операций W_b может быть представлен выражением:

$$W_b = 1 - \frac{\sum_{j \in B} P_j \sum_{i \in N_j} \lambda_{ij} t_j (1 - m_i)}{\sum_{j \in B} P_j \sum_{i \in N_j} \lambda_{ij} t_j} \qquad (2)$$

где N_j- количество наиболее вероятных информационных угроз для j-го бизнес-процесса, связанного с утечкой информации;

m_i - коэффициент защищенности, показывающий, какой каналутечки i-го вида выявляется за счет применения DLP-системы;

λ_{ij}- интенсивность возможных утечек информациив ходе j-гобизнес-процесса $(i \in N_j)$, для $i \notin N_j$, $\lambda_{ij} = 0$;

t_j - время выполнения j-ой бизнес–операции;

B - количество бизнес - операций в бизнес-процессе;

P_j - вероятность выполнения бизнес-операцийjв бизнес-процессе B.

Для проведения экспериментальной оценки эффективности DLP-решения необходимо смоделировать ситуации передачи конфиденциальной информации, в различных форматах, по различным каналам связи.

На рис. 2 представлена искомая структурная модель оценки эффективности DLP- решения. Каналы перехвата информации, в общем случае, можно разделить на внутренние и внешние. К внутренним каналам относятся каналы, сформированные при передаче информации между персональными компьютерами в локальной сети предприятия и внешними носителями, функционирующими в

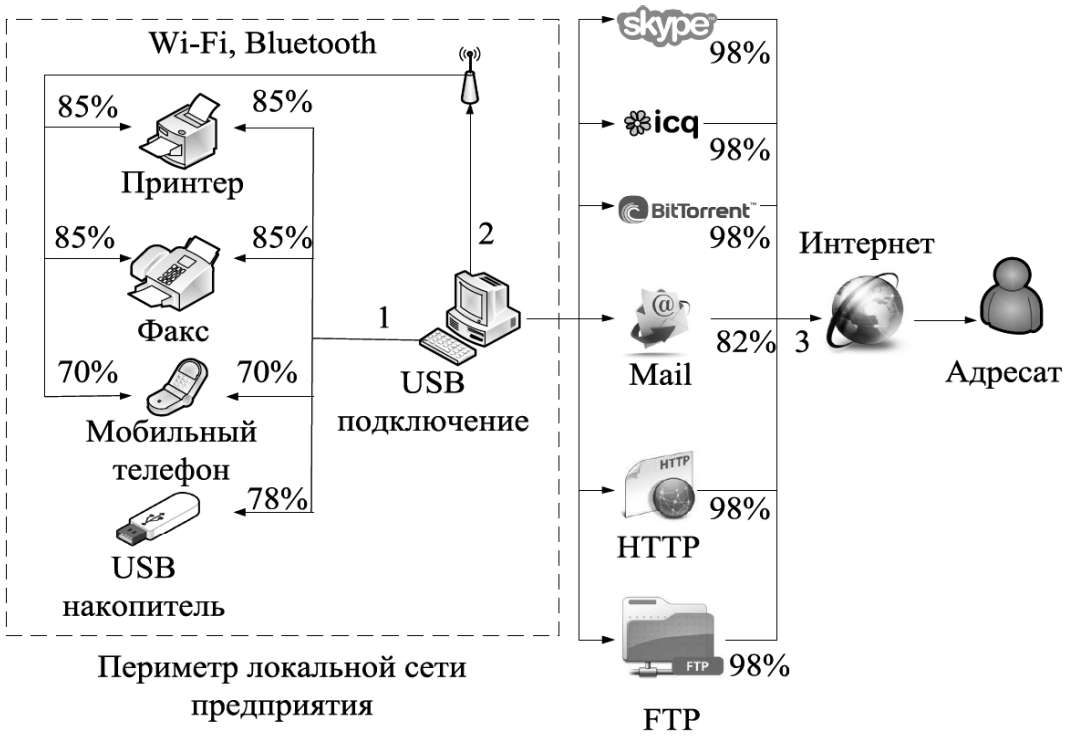

Рис. 2. Структурная модель оценки эффективности DLP-систем

пределах локальной сети (USB-накопители, сетевые принтеры и факсы). Взаимодействия по проводным и беспроводным каналам локальной сети показаны на рис. 2 стрелками 1 и 2, соответственно.

К внешним каналам целесообразно отнести почтовые сервисы, наиболее популярные мессенджеры, такие как Skype, ICQ, облачные сервисы и torrent. Передачу данных через сеть международного информационного обмена обозначены стрелкой 3.

Для проведения количественной оценки эффективности DLP-системы с использованием разработанной модели, необходимо задать допустимые параметры обнаружения утечек информации по каналу. Допустимые параметры обнаружения утечек информации по каналу определяются, как процентное соотношение выявленных утечек ко всем утечкам по каналу, при котором защита канала будет считаться эффективной. Минимальные допустимые параметры обнаружения утечек информации по различным каналам выберем на основании статистики по каналам утечек за первое полугодие 2016 года[8], основываясь на следующем принципе: чем больше процент утечек по данному каналу, тем выше должен быть минимальный допустимый параметр обнаружения утечек.

Экспериментальная оценка эффективности реагирования DLP-системы на инциденты предполагает реализацию следующей последовательности действий:

1. Настройка политики реагирования на инциденты в соответствии с руководством администратора к конкретной DLP-системе.

2. Имитирование нарушения политики безопасности (инцидента безопасности), посредством отправки конфиденциальной информации по случайно выбранному каналу связи.

3. Оценка адекватности реагирования DLP-системы, с регистрацией следующих событий:

- обнаружение инцидента безопасности;
- определение источника утечки информации;
- действия по блокированию канала утечки.

Этот перечень действий необходимо провести для каждого регулируемого канала информационного взаимодействия и провести суммарную оценку эффективности реагирования DLP-системы. Для проведения количественной оценки, с учетом имитирования протекающих в информационной системе бизнес-процессов предполагается использо-

вание выражений (1,2). На основании данной модели целесообразно дальнейшее проведение практических исследований эффективности работы DLP-систем.

Таким образом, анализ критериев оценки эффективности DLP-систем позволил осуществить сравнение нескольких наиболее известных решений на соответствие заданным критериям. Разработанная модель оценки эффективности применения DLP-систем позволяет оптимизировать процесс выбора наилучшего решения для корпоративной сети на основании задаваемых критериев оценки, что, в конечном итоге способствует повышению уровня защищенности информационных систем на практике.

Примечания

1. Утечка информации – современная угроза бизнесу// Журнал «InformationSecurity/ Информационная безопасность», №5 2011. URL: http://www.itsec.ru/articles2/Oborandteh/ytechka-informacii-sovremennaya-ygroza-biznesy (дата обращения: 1.11.2016).

2. Обзор решений для защиты от утечек информации// Журнал «InformationSecurity/ Информационная безопасность», №3 2016. URL: http://www.itsec.ru/imag/insec-3-2016/ (дата обращения: 1.11.2016).

3. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP – системы на основе FalcongazeSecureTower // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – Пермь, 2015. - № 16. – С. 57 - 67.

4. 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.

5. 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.

6. Персональный сайт компании TopSBusinessIntegrator [Электронный ресурс]. 2001 – 2012. URL: http://www.topsbi.ru/default.asp?trID=1206 (дата обращения: 3.11.2016).

7. Кумунжиев К.В., Зверев И.Н. Метод повышения эффективности dlp-системы при семантическом анализе и категоризации информации // Современные проблемы науки и образования. – 2014. – № 5. URL: http://www.science-education.ru/ru/article/view?id=14741 (дата обращения: 13.11.2016).

8. Исследование утечек информации в первом полугодии 2016 года [Электронный ресурс]. – URL: https://www.infowatch.ru/report2016_half (дата обращения: 16.11.2016).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета, 614990, Пермь, Комсомольский пр., 29. E-mail: shans@at.pstu.ru.

ЖУРИЛОВА Елена Евгеньевна, студент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета, 614990, Пермь, Комсомольский пр., 29. E-mail: ele11485995@yandex.ru.

SHABUROV AndreySergeevich, PhD of Technical Sciences at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: shans@at.pstu.ru.

ZHURILOVA Elena Evgen'evna, student at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, 614990, 29, Komsomolsky prospect, Perm. E-mail: ele11485995@yandex.ru.