УДК 004.056.5

Т. А. АНДРИЯНОВА, С. Б. САЛОМАТИН

ИСПОЛЬЗОВАНИЕ АДАПТИРОВАННОЙ DLP-СИСТЕМЫ ДЛЯ БЛОКИРОВАНИЯ УТЕЧЕК ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники

Исследуется важность использования адаптированной DLP-системы в режиме «Блокирования» утечек конфиденциальной информации компании. Приведена схема перехвата событий информационной безопасности в режиме «Копирования», анализ которой отражает главный недостаток использования данного режима – работа DLP-системы происходит только с копиями конфиденциальных документов, в то время как оригиналы доставляются получателю. Такие случаи наносят компаниям огромный ущерб, поэтому передача особо критичной информации за пределы корпоративной сети является недопустимой.

Предложено решение по переходу работы DLP-системы из режима «Копирования» в режим «Блокирования». Важно, чтобы работа DLP-системы не затрудняла выполнение сотрудниками компании штатных операций и не тормозила бизнес-процессы. Поэтому обязательным является проведение адаптации стандартной DLP-системы к специфике деятельности компании. После проводится переход адаптированной DLP-системы в режим «Блокирования».

Разработаны: процедура перехода адаптированной DLP-системы из режима «Копирования» в режим «Блокирования», схемы перехвата событий DLP-системой для двух режимов. Проведено исследование основных каналов утечки конфиденциальной информации, выделены главные утечки по типу данных и по каналу передачи. Проведен анализ работы DLP-системы в режим «Блокирования» и сделаны выводы о необходимости такого перехода.

Ключевые слова: *информационная безопасность; DLP-система; блокирование утечек информации; событие информационной безопасности; защита конфиденциальной информации; детектирование информации.*

Введение

Главным показателем полнофункциональной DLP-системы является качество решения ключевой для таких систем задачи – предотвращение утечки конфиденциальной информации. Однако, на сегодняшний день менее 50% компаний, которые используют DLP-системы в качестве элемента комплекса защиты информации, осуществили переход работы DLP-системы из режима «Копирования» в режим «Блокирования» утечек конфиденциальной информации. Такие компании не уверены в точности классификации конфиденциальной информации своей DLP-системой и опасаются нарушения бизнес-процессов компании. Работа DLP-системы в режиме «Копирования» не предотвращает выход конфиденциальных данных за пределы компании, а лишь указывает на свершенные инциденты информационной безопасности.

Решением проблемы перехода работы DLP-системы в режим «Блокирования» является адаптивная настройка DLP-решения. Процедуры адаптации стандартной DLP-системы к специфике работы корпоративной сети исследовались в работе «DLP: снижение риска утечки конфиденциальной информации Банка» [1]. Результаты работы адаптированной DLP-системы доказывают, что настройка системы в соответствии со спецификой работы корпоративной сети значительно снижает количество ложных срабатываний, повышая точность детектирования конфиденциальной информации и снижая риск утечки критичной информации за пределы корпоративной сети.

В настоящем исследовании описывается работа адаптированной DLP-системы в режиме «Блокирования» попыток нелегитимной передачи конфиденциальной информации. Разработана процедура перехода DLP-системы из режима «Копирования» в режим «Блокирования», схемы перехвата событий DLP-системой для двух режимов, исследуются основные ка-

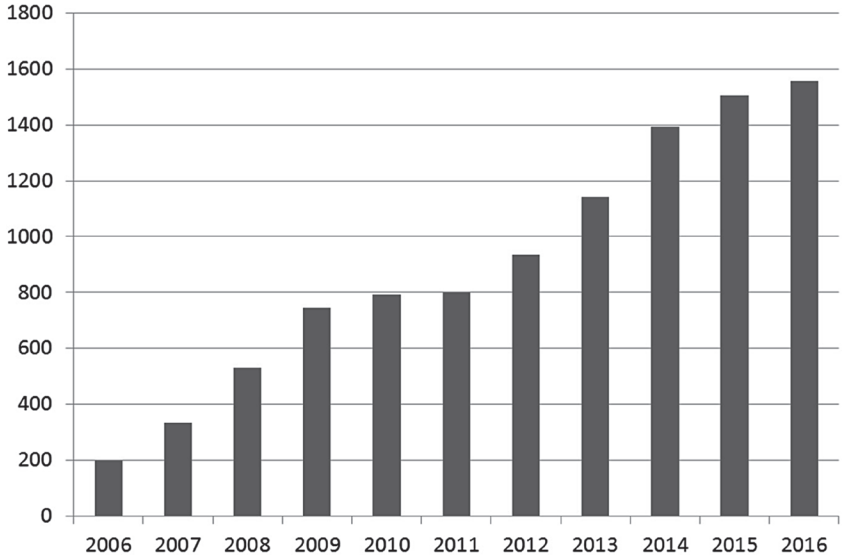

Рис. 1. Статистика количества утечек информации по годам

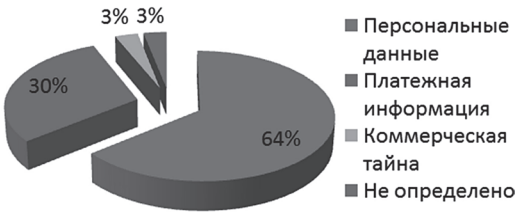

Рис. 2. Распределение утечек по типам данных

налы утечек информации, проводится анализ работы DLP-системы в режим «Блокирования».

Главные каналы утечки информации

Согласно данным аналитического центра компании InfoWatch за 2017 год, количество утечек конфиденциальной информации растет с каждым годом. В 2016 году было зафиксировано на 3,4% случаев утечки конфиденциальной информации больше, чем в 2015 году по всему миру [2]. Данные статистики отображены на рис. 1.

Согласно данным отчета об утечках конфиденциальной информации аналитического центра Zecurion Analytics, наиболее популярным каналом утечек информации на сегодняшний день стали веб-сервисы. В среднем с ними связано около четверти всех публичных инцидентов [3]. Данные аналитических отчетов центра Zecurion показывают, что больше всего инцидентов информационной безопасности связано с использованием электронной почты и копированием информации на внешние носители.

Последние данные аналитического центра компании InfoWatch за 2017 год: в 30% случаев была скомпрометирована именно платежная информация, а 64% инцидентов связаны с утечкой персональных данных [2].

Анализ представленных выше данных позволяет сделать вывод, что наибольший интерес злоумышленников представляют «Персональные данные», «Платежная информация» и «Коммерческая тайна». А главными каналами утечки данных являются: использование электронной почты и внешних носителей информации.

Анализ статистики позволяет утверждать, что использование DLP-системы в банковском сегменте является необходимым. Но так как ущерб от потери критичной информации часто не поддается подсчету, то не достаточно только знать о том, что конфиденциальная информация покинула пределы корпоративной сети, но и блокировать каналы утечки.

Адаптированная DLP-система с режимами «Копирования» и «Блокирования»

На рис. 3 представлена общая схема перехвата событий DLP-системой в режиме «Копирования».

В режиме «Копирования» DLP-система только получает копии объектов. Отличие ре-

Рис. 3. Схема перехвата событий DLP-системой в режиме «Копирования»

жима «Копирования» от режима «Блокирования» заключается в том, что транспортировка объектов выполняется без участия DLP-системы. Таким образом, задачей DLP-системы является только анализ объектов. Поскольку анализ выполняется для копии объекта, то вердикт и решение пользователя, вынесенные по результатам анализа, не оказывают влияния на доставку этого объекта получателям [4].

Для перехода работы DLP-системы в режим «Блокирования» утечки информации, необходимо осуществить классификацию информационных ресурсов компании по критерию принадлежности – составить «Перечень информации ограниченного распространения компании». Далее проводится процедура перехода адаптированной DLP-системы в режим «Блокирования». Данная процедура состоит из следующих этапов:

1. Разработка алгоритмов управления DLP-системой компании – совокупность правил, в соответствии с которыми проводится анализ и обработка объектов перехвата.

2. Разработка периметров компании – создание маршрутов легитимной и нелегитимной передачи конфиденциальной информации.

3. Определение вердиктов для каждой категории нарушения – заключение о наличии или отсутствии нарушений в анализируемом событии, а также определение возможности дальнейшей транспортировки события.

4. Оценка точности детектирования информации согласно разработанным алгоритмам управления. Для тех правил, которые срабатывают практически безошибочно и редко меняются (при условии согласования рисков), вводим режим «Блокирования».

Схема перехвата событий информационной безопасности DLP-системой в режиме «Блокирования» представлена на рис. 4.

Адаптированная DLP-система анализирует сетевой и почтовый трафики. В зависимости от наличия нарушений, возможны следующие варианты движения трафика:

- если нарушение отсутствует, на прокси-сервер возвращается сообщение, разрешающее передачу трафика. Далее трафик от прокси-сервера направляется к следующему звену сети, в зависимости от инфраструктуры компании;

- если обнаруживается нарушение, на прокси-сервер возвращается сообщение, запрещающее передачу трафика. Трафик блокируется, а пользователь, отправивший трафик, получает сообщение с предупреждением.

Специалисты службы информационной безопасности компании имеют возможность доставки объекта получателю после блокирования данного сообщения. Данная возможность определяется выставлением вердикта, вынесенным по объекту. Возможные значения:

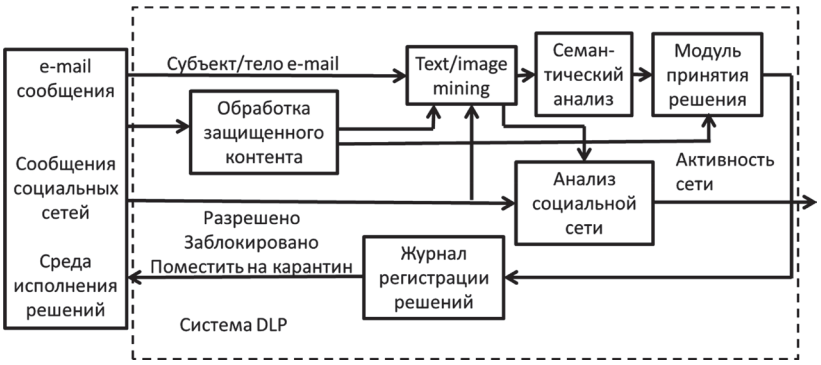

Рис. 4. Схема перехвата событий DLP-системой в режиме «Блокирования»

«Разрешено» – объект не является потенциальным нарушением и может быть доставлен получателям.

«Заблокировано» – объект является потенциальным нарушением. В режиме «Блокирования» доставка такого объекта блокируется.

«Поместить на карантин» – требуется решения пользователя, является ли объект нарушением. В режиме «Блокирования» доставка такого объекта откладывается до вынесения решения специалистом службы информационной безопасности. В зависимости от решения пользователя значение вердикта изменится либо на «Разрешено» (в этом случае выполняется доставка), либо на «Заблокировано».

Для анализа данных при попытке их отправки с компьютера сотрудника, DLP-система использует технологии лингвистического анализа, детектирования текстовых объектов, а также технологию комбинированных объектов защиты, что позволяет распознать сложные структуры данных, исключить ложные срабатывания и обеспечить высокую точность срабатывания, не нарушая работу бизнес-процессов компании [5–9].

Работа адаптированной DLP-системы в режиме «Блокирования» утечек информации позволяет специалистам службы информационной безопасности предотвращать внутренние угрозы сети непосредственно в момент их реализации. Повышение точности классификации конфиденциальных данных существенно облегчает работу службы информационной безопасности благодаря сокращению временных ресурсов, необходимых на эксплуатацию системы.

Заключение

Работа DLP-системы в режиме «Копирования» не имеет технической возможности предотвращения утечки информации. В результате, многие утечки конфиденциальной информации не пресекаются, а расследуются постфактум, что может привести к существенным потерям. Применение двухрежимной адаптированной DLP-системы позволит реализовать функции анализа, обнаружения и блокирования каналов утечки информации в корпоративных сетях.

Литература

1. **Андриянова, Т. А.** DLP: снижение риска утечки конфиденциальной информации Банка / Т. А. Андриянова, С. Б. Саломатин // Системный анализ и прикладная информатика. – 2017. -№ 3.

2. **Аналитический** центр компании InfoWatch / InfoWatch [Электронный ресурс]. – 2017. – Режим доступа: https:/ www.infowatch.ru/analytics. – Дата доступа: 04.09.2017.

3. **Аналитический** центр компании Zecurion Analytics / Zecurion [Электронный ресурс]. – 2017. – Режим доступа: http://www.zecurion.ru/press/analytics/. – Дата доступа: 30.08.2017.

4. **Техническая** база знаний компании InfoWatch / InfoWatch [Электронный ресурс]. – 2017. – Режим доступа: https:// kb.infowatch.com/#all-updates. – Дата доступа: 11.08.2017.

5. **Петраков, А. В.** Основы практической защиты информации. / А. В. Петраков //: учеб. пособие. – М.: 2005. – 281 с.

6. **Зегжда, Д. П.** Основы безопасности информационных систем / Зегжда, Д. П., Ивашко, А. М. // М.: Горячая линия – Телеком, 2000. – 452 с.

7. **Мелюк, А. А.** Введение в защиту информации в автоматизированных системах / А. А. Мелюк, С. В. Пазизин, Н. Погожин // М.: Горячая линия – Телеком, 2001. – 48с.

8. **Батаронов, И. Л.** Оценка и регулирование рисков, обнаружение и предупреждение компьютерных атак на инновационные проекты / И. Л. Батаронов, А. В. Паринов, К. В. Симонов // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 243–246 с.

9. **Бутузов, В. В.** К вопросу обоснования функции ущерба атакуемых систем / В. В. Бутузов, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 47–54.

References

1. **Andrijanova, T. A.** DLP: snizhenie riska utechki konfidencial'noj informacii Banka / T. A. Andrijanova, S. B. Salomatin // Sistemnyj analiz i prikladnaja informatika. – 2017. -№ 3.

2. **Analiticheskij** centr kompanii InfoWatch / InfoWatch [Jelektronnyj resurs]. – 2017. – Rezhim dostupa: https://www.infowatch.ru/analytics. – Data dostupa: 04.09.2017.

3. **Analiticheskij** centr kompanii Zecurion Analytics / Zecurion [Jelektronnyj resurs]. – 2017. – Rezhim dostupa: http://www.zecurion ru/press/analytics/. – Data dostupa: 30.08.2017.

4. **Tehnicheskaja** baza znanij kompanii InfoWatch / InfoWatch [Jelektronnyj resurs]. – 2017. – Rezhim dostupa: https://kb.infowatch.com/#all-updates. – Data dostupa: 11.08.2017.

5. **Petrakov, A. B.** Osnovy prakticheskoj zashhity informacii. / A. B. Petrakov //: ucheb. posobie. – M.: 2005. – 281 c.

6. **Zegzhda, D. P.** Osnovy bezopasnosti informacionnyh sistem / Zegzhda, D. P., Ivashko, A. M. // M.: Gorjachaja linija – Telekom, 2000. – 452 s.

7. **Meljuk, A. A.** Vvedenie v zashhitu informacii v avtomatizirovannyh sistemah / A. A. Meljuk, S. V. Pazizin, N. Pogozhin // M.: Gorjachaja linija – Telekom, 2001. – 48 s.

8. **Bataronov, I. L.** Ocenka i regulirovanie riskov, obnaruzhenie i preduprezhdenie komp'juternyh atak na innovacionnye proekty / I. L. Bataronov, A. V. Parinov, K. V. Simonov // Informacija i bezopasnost'. – 2013. – T. 16. – Vyp. 2. – S. 243–246 c.

9. **Butuzov, V. V.** K voprosu obosnovanija funkcii ushherba atakuemyh sistem / V. V. Butuzov, A. V. Zarjaev // Informacija i bezopasnost'. – 2013. – T. 16. – Vyp. 1. – S. 47–54.

Поступила	*После доработки*	*Принята к печати*
18.09.2017	*26.09.2017*	*15.12.2017*

Andryianava T. A., Salomatin S. B.

USING THE ADAPTED DLP SYSTEM FOR BLOCKING INFORMATION LEAKS

The importance of using the adapted DLP-system in the «Blocking» mode of leaking confidential information of the company is investigated. The scheme of interception of information security events in the «Copy» mode is given, the analysis of which reflects the main drawback of using this mode – the DLP-system works only with copies of confidential documents, while the originals were delivered to the recipient. Such cases inflict enormous damage on companies, so the transfer of critical information beyond the corporate network is unacceptable.

A solution is proposed for transferring the operation of the DLP-system from the «Copy» mode to the «Blocking» mode. It is important that the operation of the DLP-system does not hinder the staff members from performing regular operations and does not hinder business processes. Therefore, it is mandatory to adapt the standard DLP-system to the specifics of the company's activities. After that the transition of the adapted DLP-system to the «Blocking» mode is carried out.

Developed: the transition procedure of the adapted DLP-system from the «Copy» mode to the «Blocking» mode, the scheme of the event capture by the DLP-system for the two modes. The main channels of data leaks were investigated, the main leaks were identified by the data type and by the transmission channel. The analysis of the DLP-system operation in the «Blocking» mode is performed.

Keywords: *information security; DLP-system; blocking of information leaks; an information security event; protection of confidential information; information detection.*

Андриянова Т. А., аспирант Белорусского государственного университета информатики и радиоэлектроники. Окончила Белорусский государственный университет информатики и радиоэлектроники по специальности «Радиоэлектронная защита информации» в 2009 году, магистратуру по специальности «Методы и системы защиты информации, информационная безопасность» в 2010.

220013, Республика Беларусь, Минск, ул. П. Бровки, 6, Белорусский государственный университет информатики и радиоэлектроники.

Тел: + 375293436560; e-mail: rezistka@gmail.com

Andryianava T. A., postgraduate student of Belarusian state university of informatics and radioelectronics. Graduated from Belarusian state university of informatics and radioelectronics «Radioelectronic information security» 2009, Master of Technical Sciences «Methods and systems of information security, information security» 2010.

Саломатин С. Б., к. т. н., доцент Белорусского государственного университета информатики и радиоэлектроники.

Тел: + 375296714732; e-mail: kafsiut@bsuir.by

Salomatin S. B., Ph. D., associate professor of Belarusian state university of informatics and radioelectronics.