УДК 004.056.5

Т. А. АНДРИЯНОВА, С. Б. САЛОМАТИН

DLP: СНИЖЕНИЕ РИСКА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ БАНКА

Белорусский государственный университет информатики и радиоэлектроники

Исследуется применение DLP-системы для защиты конфиденциальной информации, предлагается методика адаптации DLP-системы к специфике деятельности организации, проводится сравнительный анализ результатов работы стандартной и адаптированной DLP-систем в Банке. Разработаны: методика анализа событий информационной безопасности, алгоритм реагирования на выявленные события, а также методика и процедуры адаптации стандартной DLP-системы к специфике деятельности Банка. Методика адаптации стандартной DLP-системы к специфике работы Банка состоит из следующих мероприятий: определение категорий критичной корпоративной информации, аудит информационных систем, описание актуальных рисков и их оценка, введение регламентов обращения с информацией ограниченного распространения и настройку DLP-системы в соответствии со спецификой работы Банка. Модернизация конфигурации стандартной DLP-системы включает в себя следующие процедуры: селекцию конфиденциальной информации Банка по критерию принадлежности, настройку детектирования, создание периметров и разработку алгоритма реагирования на выявленные события информационной безопасности в Банке. Алгоритм предназначен для повышения эффективности реагирования сотрудниками службы информационной безопасности в случаях выявления инцидентов и описывает этапы последующих действий. Результаты исследований доказывают, что использование адаптированной DLP-системы значительно снижает количество ложных срабатываний, повышая точность детектирования конфиденциальной информации и снижая риск утечки критичной информации за пределы корпоративной сети. Применение адаптированной DLP-системы в Банке позволило повысить быстродействие реагирования специалистов службы информационной безопасности на выявленные адаптированной DLP-системой события информационной безопасности в Банке, а также позволило осуществить переход работы DLP-системы из режима копирования в режим блокирования нелегитимной передачи информации.

Ключевые слова: *Информационная безопасность; DLP-система; система мониторинга; событие информационной безопасности; утечка конфиденциальной информации; детектирование информации; алгоритм реагирования на инциденты.*

Введение

Деятельность банков всегда была связана с обработкой и хранением большого количества конфиденциальных данных. Поэтому на первый план выходят риски, связанные с утечкой конфиденциальной информации. Прежде всего, для защиты от утечек конфиденциальной информации применяются DLP-системы.

DLP-системы – это системы защиты конфиденциальной информации, которые отслеживают и анализируют данные, отправляемые за пределы организации через корпоративную и веб-почту, Интернет (в том числе и по защищенному протоколу HTTPS), а также системы мгновенного обмена сообщениями и Skype. Данные системы также позволяют сотрудникам службы безопасности контролировать отправку файлов на принтеры и копирование информации на съемные носители [1].

В настоящей работе приводятся результаты исследования адаптации DLP-системы в Банке для проведения мониторинга информационной безопасности.

Стандартная DLP-система

Стандартная DLP-система (DLPs) позволяет контролировать информационные потоки в корпоративной среде для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных. Структурная схема DLPs представлена на рис. 1.

Для контроля утечек информации используются «Технологии» – набор инструментов анализа, выполняющих поиск заданных эле-

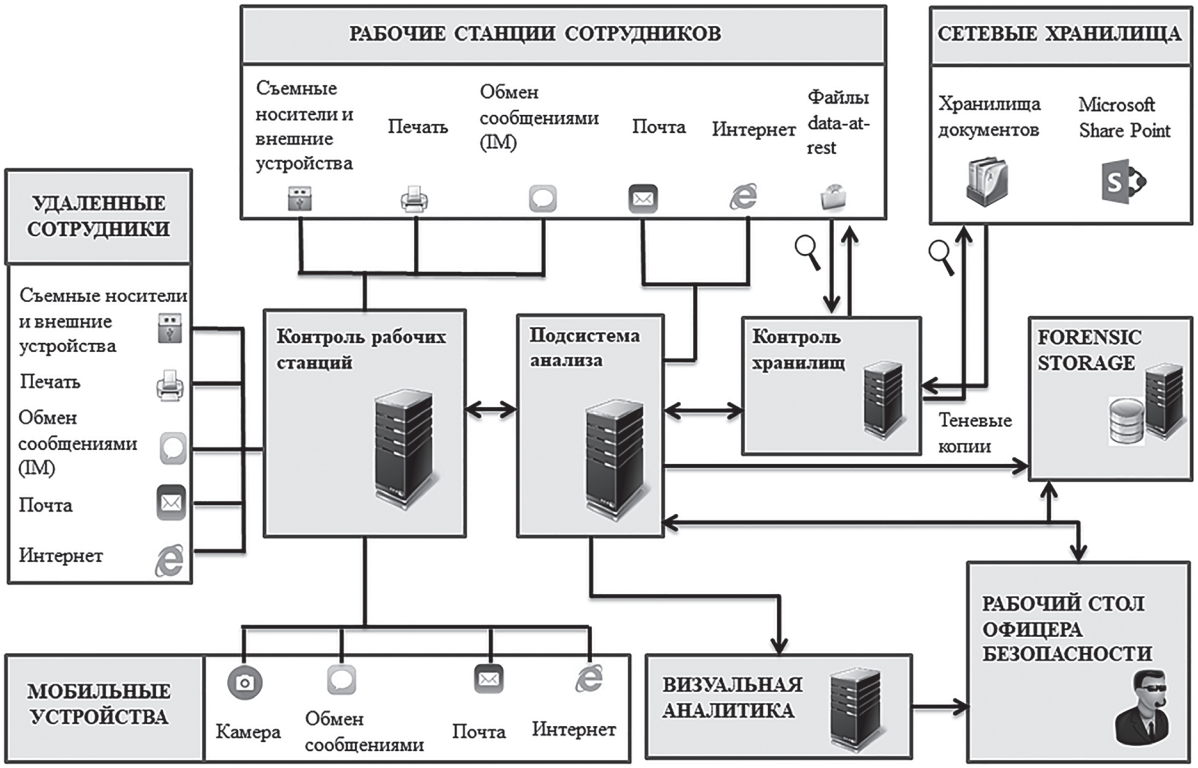


Рис. 1. Структурная схема DLPs

ментов в контексте событий информационной безопасности. Событие – объекты перехвата трафика (SMTP-, IMAP-, POP3-письма, HTTP-запросы, ICQ-сообщения, Skype-сообщения), теневые копии файлов и задания на печать, которые создаются DLPs в результате обмена данными между сотрудниками компании и другими организациями, включая публикацию в общедоступных источниках, копирование на внешние устройства и печать.

«Технологии» состоят из категории и терминов, эталонных документов, бланков, выгрузок, текстовых и графических объектов, и представляют собой пример конфиденциальных данных организации.

Контекст события – внутреннее представление перехваченного события – XML данные, извлеченные из события и его вложений. После обработки с помощью «Технологий» к контексту добавляются результаты анализа и информация о решении по событию [2–3].

Обработка и анализ перехваченных DLPs объектов осуществляется подсистемами, представленными в таблице.

Методика анализа событий информационной безопасности выполняется в следующем порядке:

1. Выделение атрибутов – подсистема Обработки выделяет у объектов имеющиеся атрибуты (у SMTP-писем – адреса отправителя и получателей, тема письма и т. п.).

2. Извлечение вложенных файлов – модуль Принятия решений анализирует вложенные файлы на основании названия и формата файла.

3. Анализ текста и графических объектов – подсистема Анализа обрабатывает текстовые и графические данные: тексты писем, сообщений, запросов; тексты, извлеченные из вложений поддерживаемых форматов, а также файлы изображений.

На основании результатов анализа модуль Принятия решений выносит заключение о возможном нарушении правил информационной безопасности и определяет, какие действия должны быть выполнены в случае нарушения.

Однако стандартная DLP-система имеет ряд недостатков:

1. Огромное количество ложных срабатываний. Так как DLPs внедряется со стандартными настройками, то она содержит множество загруженных категорий и классов конфиденциальности, тем самым увеличивая количество детектируемых документов.

Подсистемы обработки и анализа перехваченных DLPs объектов

Подсистема	Модули подсистемы	Функции подсистемы/модуля
Обработки	Обработки SMTP- и POP3-трафика Обработки HTTP-трафика Обработки ICQ-трафика Обработки Теневых Копий Обработки SMTP-трафика Обработки HTTP-трафика	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в подсистему Анализа.
Анализа	Лингвистического анализа	Проверка текста на соответствие каким-либо категориям.
	Детектирования текстовых объектов	Поиск текстовых объектов (например, номеров кредитных карт) в тексте объектов.
	Детектирования цифровых отпечатков	Поиск цитат из эталонных документов в тексте объектов.
	Детектирования бланков	Поиск бланков в тексте объектов.
	Детектирования печатей	Поиск изображений печатей в тексте объектов.
	Детектирования выгрузок из БД	Поиск цитат из базы данных в тексте событий.
	Детектирования графических объектов	Поиск изображений, принадлежащих определенным классам, в тексте и вложениях объектов.
Применения алгоритмов управления	Принятия решений	Обеспечение корпоративной политики безопасности путем выполнения для объектов правил из набора алгоритмов управления.

2. Из первого недостатка следует второй – увеличение ресурсов, необходимых на эксплуатацию системы.

3. Невозможность использования DLPs в режиме блокировки утечек. На сегодняшний день все стандартные DLP-системы работают в режиме копирования, т. к. организации, их использующие, опасаются нарушения своих бизнес-процессов. В результате, многие утечки информации не пресекаются, а расследуются постфактум, и компании всё равно несут потери.

«Технологии» DLP-систем дают возможность с высокой точностью детектировать конфиденциальную информацию и определять тематику документов и сообщений, передаваемых за пределы организации, только в том случае, когда был проведен процесс адаптации DLPs и модернизация стандартных технологий под нужды компании.

Адаптивная DLP – система Банка

Службой безопасности Банка проводится мониторинг информационной безопасности с помощью DLP-системы. Офицер службы безопасности Банка проводит постоянное наблюдение за объектами и субъектами, действиями и процессами, влияющими на информационную безопасность, а также регистрацию, сбор, анализ и обобщение результатов наблюдений.

Для устранения недостатков работы стандартной DLPs и автоматизации ее работы, был осуществлен процесс адаптации DLP-системы.

Ниже представлена разработанная методика адаптации DLPs к специфике работы Банка. Данная методика состоит из следующих мероприятий:

1. Определение категорий критичной корпоративной информации и составление «Перечня информации ограниченного распространения Банка».

2. Аудит информационных систем – описание путей распространения информации внутри Банка, фиксирование ее владельцев и мест хранения.

3. Описание актуальных рисков, оценка рисков утечки информации.

4. Введение регламентов обращения с информацией ограниченного распространения.

5. Настройка DLP-системы в соответствии со спецификой работы Банка – обучение системы различать конфиденциальную информацию в потоке трафика и отличать, когда передача конфиденциальной информации осуществляется легитимно.

Для создания адаптивной DLP-системы (DLPa) была выполнена модернизация конфигурации БКФ. Данные изменения включают в себя следующие процедуры:

1. Селекция конфиденциальной информации Банка по критерию принадлежности. Каждый документ Банка, содержащий информацию ограниченного распространения отнесен

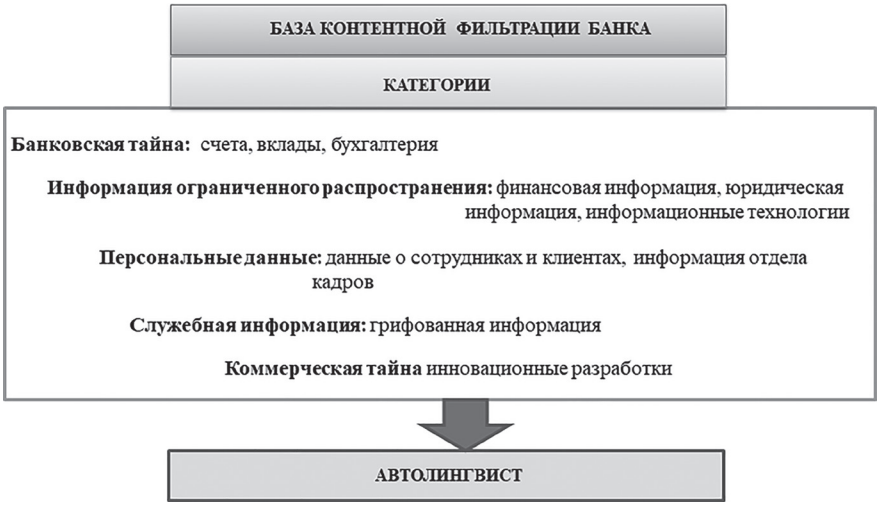


Рис. 2. База контентной фильтрации

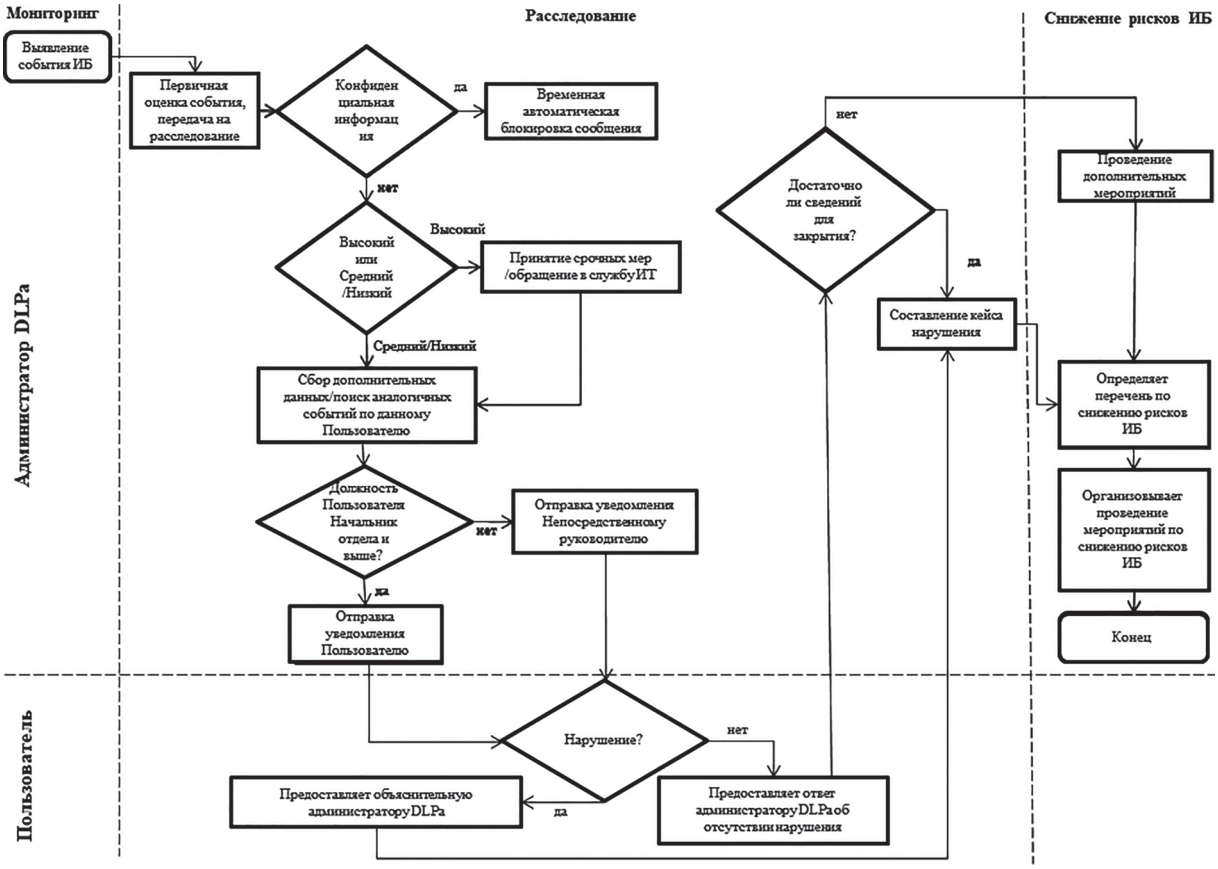
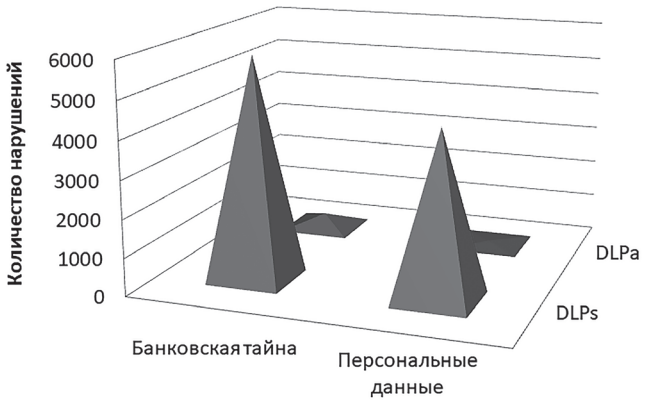


Рис. 3. Алгоритм реагирования на выявленные события

к конкретному пункту «Перечня информации ограниченного распространения Банка» и на его основе создана База контентной фильтрации (БКФ). БКФ представляет собой иерархически организованный список категорий и содержит слова и выражения, наличие которых в документе позволяет определить тематику и степень конфиденциальности информации. Банковская БКФ представлена на рис. 2.

2. Настройка детектирования: заполнение «Технологий» DLPa, создание объектов защиты и формирование алгоритмов управления DLPa. В модули подсистемы Анализа DLPa импортированы шаблоны документов, содержащих информацию ограниченного распространения Банка: бланки договоров, изображения печатей Банка и кредитных карт, текстовые объекты номеров счетов и реквизиты па-



	Банковская тайна	Персональные данные
DLPs	5874	4401
DLPa	364	70

Рис. 4. Статистика перехваченных DLPs и DLPa событий

спорта. Также выстроены связи между объектами и субъектами системы мониторинга событий информационной безопасности.

Для DLPa на основании множества документов, подпадающих под один и тот же пункт «Перечня информации ограниченного распространения Банка», сформированы правила при помощи выставления весов, которые позволяют автоматически определить пункт перечня, к которому относится детектируемый документ. Когда сумма весов в документе превышает установленный порог либо соотношение частоты встречаемости ключевых слов близко к соотношению их весов, происходит срабатывание. Большой вес получают слова с высокой частотой в пределах конкретного документа и с низкой частотой употреблений в других документах [4].

3. Создание периметров. Проработка возможных ситуаций передачи информации и создание периметров, создание маршрутов легитимной передачи конфиденциальной информации, выставление исключений по периметрам внутри Банка.

4. Разработка алгоритма реагирования на выявленные события информационной безопасности в Банке. Данный алгоритм включает в себя этапы мониторинга, расследования инцидентов информационной безопасности и процедуры снижения рисков информационной безопасности. Алгоритм реагирования на выявленные события представлен на рис. 3.

Алгоритм предназначен для повышения эффективности реагирования сотрудниками службы информационной безопасности в случаях выявления инцидентов и описывает этапы последующих действий [5–8].

Результаты работы адаптивной DLP-системы

Для оценки работы адаптивной DLPa были сформированы и проанализированы два отчета. Первый отчет был сформирован при детектировании объектов защиты «Банковская тайна» и «Персональные данные» за 7 дней для DLPs при стандартных настройках DLP-системы. Второй отчет сформирован при детектировании тех же объектов защиты «Банковская тайна» и «Персональные данные» за 7 дней, но уже для DLPa после процесса адаптации DLP-системы к специфике работы Банка. Данные двух отчетов приведены на рис. 4.

Результатом работы адаптивной DLPa в Банке стало снижение ложных срабатываний DLP-системы в 16 раз при детектировании информации, содержащей персональные данные, и в 62 раза при детектировании информации, составляющей банковскую тайну. На основе полученных экспериментальных данных, можно утверждать о следующих изменениях:

1. Повышение точности детектирования конфиденциальной информации в информационном потоке.

2. Повышение быстродействия реагирования на выявленные DLPa события информационной безопасности в Банке.

3. Повышение эффективности работы DLPa в связи с возможностью перехода работы системы из режима копирования в режим блокирования нелегитимной передачи информации.

Заключение

В соответствии с полученными результатами работы, можно сделать вывод, адаптивная DLPa Банка интегрируется в существующую инфраструктуру без влияния на бизнес-процессы, стабильна в работе, проста в настройке, а главное – блокирует попытки передачи информации ограниченного распространения за пределы корпоративной сети. Тем самым, рассматриваемая DLP-система работает на снижение финансовых, репутационных и технологических рисков Банка, которые могут возникнуть в результате утечки данных.

Литература

1. **Данкевич, А.** DLP в эпоху корпоративной мобильности / А. Данкевич / Директор информационной службы № 03 [Электронный ресурс]. – 2013. – Режим доступа: https://www.osp.ru/text/print/article/13034662.html?isPdf=1. – Дата доступа:15.08.2017.

2. **Внуков, А. А.** Защита информации в банковских системах: учеб. пособие для бакалавриата и магистратуры / А. А. Внуков; М.: Издательство Юрайт, 2017. – 246 с.

3. **Технологическое** лидерство InfoWatch Traffic Monitor / InfoWatch [Электронный ресурс]. – 2017. – Режим доступа: https://www.infowatch.ru/products/traffic_monitor. – Дата доступа: 04.07.2017.

4. **Васильев, В.** DLP-системы: что нужно заказчику /В. Васильев / PC Week № 3–4 [Электронный ресурс]. – 2017. – Режим доступа: https://www.itweek.ru/security/article/detail. php?ID=192940. – Дата доступа: 02.08.2017.

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

6. **Корт, С. С.** Теоретические основы защиты информации: учеб. пособие. – М.: Гелиос АРВ, 2004. – 240 с.

7. **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.

8. **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. **Dankevich, A.** DLP v jepohu korporativnoj mobil'nosti A. Dankevich / Direktor informacionnoj sluzhby № 03 [Electronic resource]. – 2013. – Mode of access: https://www.osp.ru/text/print/article/13034662. html?isPdf=1). – Date of access: 15.08.2017.

2. **Vnukov, A. A.** Zashhita informacii v bankovskih sistemah: ucheb. posobie dlja bakalavriata i magistratury / A. A. Vnukov. M.: Izdatel'stvo Jurajt, 2017. – 246 s.(in Russ).

3. **Tehnologicheskoe** liderstvo InfoWatch Traffic Monitor / InfoWatch [Electronic resource]. – 2017. – Mode of access: https://www.infowatch.ru/products/traffic_monitor. – Date of access: 04.07.2017.

4. **Vasil'ev, V.** DLP-sistemy: chto nuzhno zakazchiku / V. Vasil'ev / PC Week № 3–4 [Electronic resource]. – 2017. – Mode of access: https://www.itweek.ru/security/article/detail.php?ID=192940. – Date of access: 02.08.2017.

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

6. **Kort, S. S.** Teoreticheskie osnovy zashhity informacii: ucheb. posobie. – M.: Gelios APB, 2004. – 240 s.

7. **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 s.

8. **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*
24.06.2017	06.07.2017	10.09.2017

T. A. Andryianava, S. B. Salomatin

DLP: REDUCED RISK OF LEAKAGE OF CONFIDENTIAL INFORMATION OF THE BANK

Research application of DLP-system for protection of confidential information, a methodology for adapting the DLP-system to the specific activities of the organization, comparative analysis of the results of standard and adapted DLP-systems in the Bank. Developed: a technique for analyzing information security events, algorithm for responding to identified events, methodology and procedures for adapting the standard DLP-system to the specifics of the Bank's activities. The methodology for adapting a standard DLP-system to the specifics of the Bank's work consists of the following activities: identification of critical corporate information categories, audit of information systems, description of current risks and their assessment, introduction of rules for Bank's critical information and setting up a DLP system in accordance with the specifics of the Bank's

work. Modernization of the configuration of a standard DLP-system includes the following procedures: selection of confidential information of the Bank based on membership criteria, setting up detection, creating perimeters and developing an algorithm for responding to identified information security events in the Bank. The algorithm is designed to improve the efficiency of the response of information security officers in cases of incident detection and describes the stages of the subsequent actions. The results of the research prove that using an adapted DLP-system significantly reduces the number of false positives, increasing the accuracy of detecting confidential information and reducing the risk of leakage of critical information outside the corporate network. The application of the adapted DLP-system in the Bank allowed to increase the speed of response of information security specialists to the information security events detected by the DLP-system adapted to the Bank, and also allowed the DLP-system to transition from the copy mode to the blocking mode of illegitimate transfer of information.

Keywords: *Information Security; DLP-system; monitoring system; an information security event; leakage of confidential information; detection of information; incident response algorithm.*

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.