DOI: 10.17117/na.2016.10.03.080

<http://ucom.ru/doc/na.2016.10.03.080.pdf>

Поступила (Received): 24.10.2016

Васильев А.Е.
Защита конфиденциальной информации
при помощи технологий DLP

Vasiliev A.E.
Protection of confidential information by using DLP technology

О защите конфиденциальных данных заговорили еще достаточно давно. Многие специалисты старались обеспечить надежную защиту важной информации. Но только с появлением современных систем надежной защиты информации DLP это стало вполне возможным на практике. Защита конфиденциальной информации при помощи технологий DLP – это очень практично, удобно и современно. Данная система дает прекрасную возможность защитить свои информационные ресурсы от взлома

Ключевые слова: информация, защита информации, конфиденциальная информация, шифрование, DLP, компьютер

Васильев Алексей Евгеньевич

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

On the protection of confidential data even talking for a long time. Many experts have tried to ensure reliable protection of important information. But only with the advent of modern systems of reliable information protection DLP it was quite possible in practice. Protection of confidential information by using DLP technology is very practical, comfortable and modern. This system provides an excellent opportunity to protect their information resources from hacking

Key words: information, data protection, confidential information, encryption, DLP, PC

Vasiliev Aleksey Evgenevich

Student

Omsk state technical university

Omsk, Mira ave., 11

На сегодняшний день защита информации при помощи систем DLP – это надежно и современно. Но первоначально с этим способом защиты данных были некоторые сложности в использовании. Защита при помощи систем DLP была надежной, но при этом персональному компьютеру было сложно определить, какая информация является конфиденциальной, а какая общедоступной для пользователей. Сейчас же система автоматически сортирует разнообразные данные на важные и не очень важные, а администратору остается только выполнить шифрование важной информации. Имеется возможность настроить персональный компьютер на высокую скорость выполнения данной операции.

Сейчас система защиты данных на базе DLP применяется для исключения утечек разнообразной информации, которую администратор может сортировать по степени важности.

Преимущества и недостатки систем защиты информации

Система защиты данных DLP имеет большое число достоинств, но также есть у нее и незначительные недостатки. Большое число производителей считает данную систему очень надежной и перспективной в развитии.

Подобные технологии можно разделить на 2 основных типа, таких как:

– Лингвистический:

Использование стоп-слов («секретно», «конфиденциально» и тому подобных) для блокировки исходящих электронных сообщений в почтовых серверах можно считать прародителем современных DLP систем. Конечно, от злоумышленников это не защищает – удалить стоп-слово, чаще всего вынесенное в отдельный гриф документа, не составляет труда, при этом смысл текста несколько не изменится. Большинство современных систем лингвистического анализа используют не только контекстный анализ (то есть в каком контексте, в сочетании с какими другими словами используется конкретный термин), но и семантический анализ текста. Эти технологии работают тем эффективнее, чем больше анализируемый фрагмент. На большом фрагменте текста точнее проводится анализ, с большей вероятностью определяется категория и класс документа. При анализе же коротких сообщений (SMS, интернет-пейджеры) ничего лучшего, чем стоп-слова, до сих пор не придумано. Автор столкнулся с такой задачей осенью 2008 года, когда с рабочих мест многих банков через мессенджеры пошли в Сеть тысячи сообщений типа «нас сокращают», «отберут лицензию», «отток вкладчиков», которые нужно было немедленно заблокировать у своих клиентов.

– Статистический:

Задача компьютерного поиска значимых цитат заинтересовала лингвистов еще в 70-х годах прошлого века, если не раньше. Текст разбивался на куски определенного размера, с каждого из которых снимался хеш. Если некоторая последовательность хешей встречалась в двух текстах одновременно, то с большой вероятностью тексты в этих областях совпадали. Статистические технологии относятся к текстам не как к связной последовательности слов, а как к произвольной последовательности символов, поэтому одинаково хорошо работают с текстами на любых языках. Поскольку любой цифровой объект – хоть картинка, хоть программа – тоже последовательность символов, то те же методы могут применяться для анализа не только текстовой информации, но и любых цифровых объектов. И если совпадают хеши в двух аудиофайлах – наверняка в одном из них содержится цитата из другого, поэтому статистические методы являются эффективными средствами защиты от утечки аудио и видео.

Эти два способа очень удобны и практичны в использовании. Но применение одного из них имеет как положительные, так и отрицательные моменты.

Одними из самых первых DLP систем многие специалисты считают использование определенных стоп-слов, которые очень быстро производят полную блокировку доступа определенных пользователей к рабочей системе с информационными данными. Но у подобного метода организации защиты данных есть недостаток. Взломщик компьютерной системы имеет возможность исключить часто используемые и распространенные в данных системах специальные стоп-слова и получить доступ к конфиденциальным данным.

Свойства информации полностью сохраняются в качественном эквиваленте и просты для использования. Если в помещении имеется звуковое устройство для прослушивания, тогда, чтобы исключить кражу информации ставится жучок, который находит устройство. Так в подобных системах и происходит определение опасности в случае защиты важных данных. Еще совсем недавно использовались специализированные e-mail фильтры. Сейчас, когда технологии значительно усовершенствовались, любой пользователь может установить антивирусную программу или программу для осуществления защиты от нежелательного спама. Подобные системы работают по технологии DLP с использованием стоп-слов, что очень удобно и практично в использовании.

Список используемых источников:

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая Линия-Телеком, 2004.
2. Астахов А. Разработка эффективных политик информационной безопасности // IT Директор. 2005.
3. Васенин В.А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности. М.: МЦНМО, 2004.

© 2016, Васильев А.Е.

Защита конфиденциальной информации при помощи технологий DLP

© 2016, Vasiliev A.E.

Protection of confidential information by using DLP technology