УДК 004.356.2

Обеспечение информационной безопасности процессов печати

А. С. Рябов
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрены вопросы обеспечения информационной безопасности процессов печати, а также проблемы, связанные с утечкой конфиденциальной информации при распечатывании документов на сетевых принтерах. Предложены применение технологии безопасной печати, позволяющей минимизировать риски информационной безопасности, путем авторизации пользователей в инфраструктуре печати.

Ключевые слова: документооборот, утечка информации, печать с авторизацией, принтер, принт-сервер, сетевой контроллер.

Часто требуется напечатать документ, содержащий конфиденциальную информацию, и очень важно, чтобы отпечатанный документ получил определенный сотрудник, а не кто-то другой. Отправив документ на сетевой принтер, расположенный в общедоступном месте, через некоторое время вы можете не найти его на выходном лотке устройства. Иногда пользователи даже просто забывают о своих распечатанных документах. В конце рабочего дня уборщица может просто собрать скопившиеся документы, которые могут содержать, в том числе, конфиденциальную информацию, и выбросить их в мусорный контейнер за пределами организации.

Разглашение содержания таких документов (персональные данные сотрудников, финансовые отчеты, информация о клиентах и партнерах и т. д.) может привести к серьезным негативным последствиям для предприятий всех уровней. Утечка информации чревата не только финансовыми потерями и юридическими последствиями, но может также привести и к потере имиджа компании и нанести серьезный урон деловой репутации. Стоит отметить, что не так давно в одном российском банке произошел очень крупный инцидент — распечатанные документы, содержащие информацию о клиентах (копии паспортов клиентов, их заявления с контактными телефонами и данными о месте жительства, работы и недвижимости), оказались на свалке.

Сегодня многие предприятия уже инвестируют в свою инфраструктуру информационной безопасности для защиты IT-систем от внешних и внутренних угроз, но мало кто из них уделяет такое же серьезное внимание вопросам защиты процессов печати, занимающей также важнейшее место в процессе создания, обработки и распространения документов. Поэтому на сегодняшний день вопросы информационной безопасности, связанные с печатью документов, остаются еще открытыми.

Самый простой путь решения данной задачи — установка персональных принтеров для сотрудников, которые работают с конфиденциальными документами. Однако таких сотрудников может быть много, а их состав и численность непостоянными. Данный способ выхода из положения становится не только очень дорогим, но и неуправляемым.

В таких случаях решением является технология безопасной печати с авторизацией, которая позволит разграничить доступ сотрудников к устройствам, распечатываемым документам, и избежать утечки информации.

Привычная для пользователя процедура печати документа выглядит следующим образом: пользователь отправляет электронный документ на определенный принтер и через какое-то время подходит к аппарату, чтобы забрать напечатанный документ. Печать документа обычно осуществляется через выделенный принт-сервер.

Решение представляет собой распределенную в ЛВС многокомпонентную систему защиты, состоящую из специализированного принт-сервера и устройства «Сетевой контроллер», которые устанавливаются в непосредственной близости к устройству печати. Распечатка документов осуществляется только после авторизации пользователя на «Сетевом контроллере». Такой механизм дает возможность визуально контролировать процесс печати и препятствует утечкам конфиденциальной информации через бумажные носители.

Рябов Андрей Сергеевич, исследователь.
E-mail: asr@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

Структурная схема компонентов системы защиты процессов печати приведена на рис. 1.

В штатном режиме традиционно после обработки задания на печать, принт-сервера посылают его на принтер или МФУ. Специализированный принт-сервер приостанавливает процесс печати до авторизации пользователя в системе защиты.

Устройство «Сетевой контроллер» с двумя сетевыми интерфейсами, предназначенное для ввода аутентификационной информации (в качестве идентификаторов могут быть использованы Touch-memory DS-199x, ПСКЗИ ШИПКА), устанавливается перед принтером или МФУ. Устройство «Сетевой контроллер» функционирует под специализированной защищенной ОС семейства Linux, которая записывается в раздел Read Only (RO). Устройство имеет два сетевых интерфейса eth0 и eth1 и является шлюзом между ЛВС и устройством печати. Интерфейс eth0 подключается к ЛВС, на нем настраивается ip-адрес принтера, поэтому нет необходимости в модификации настроек инфраструктуры печати. К интерфейсу eth1 подключается устройство печати — принтер или МФУ.

На рис. 2 изображено взаимодействие компонентов системы защиты процессов печати.

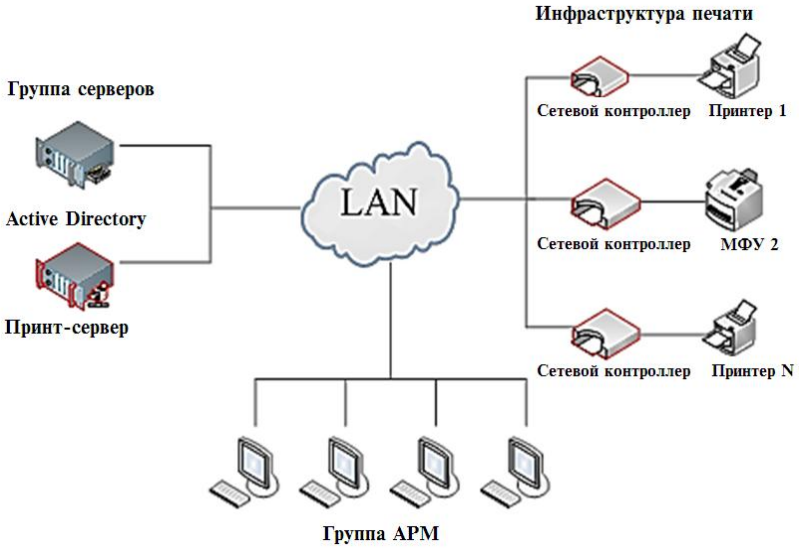

Рис. 1. Структурная схема компонентов системы защиты процессов печати

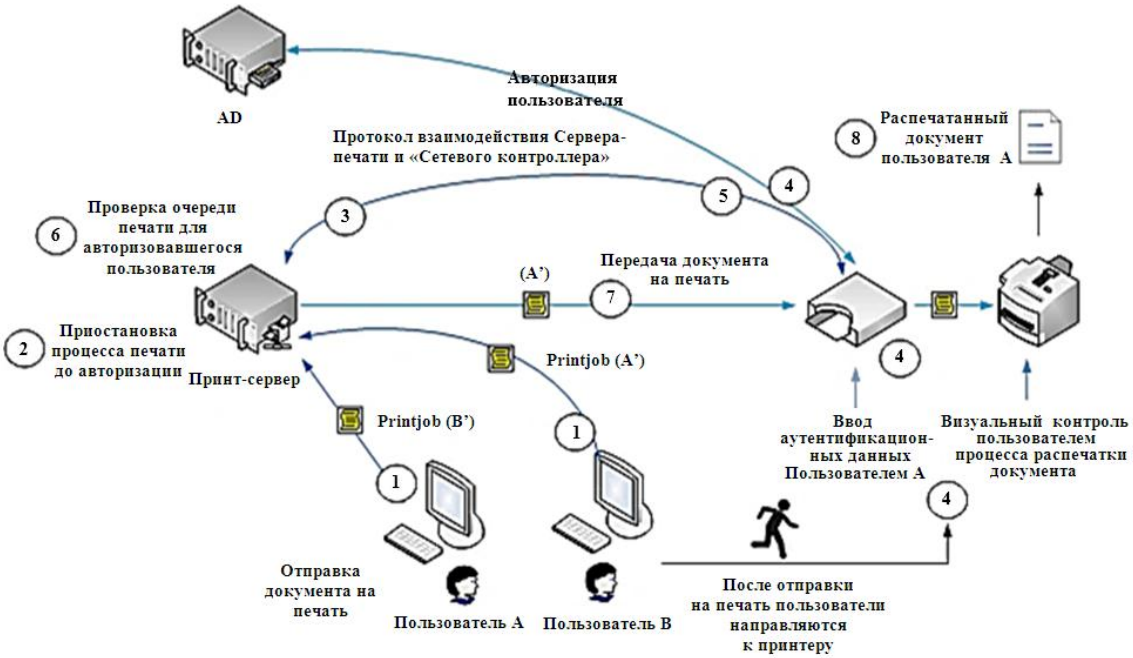

Рис. 2. Взаимодействие компонентов системы защиты процессов печати

Технологический процесс печати для двух пользователей (Пользователь А и Пользователь В) выглядит следующим образом:

1) С рабочих мест (АРМ) Пользователи А и В отправляют задания для печати Printjob (А') и Printjob (В') в очередь на принт-сервер.

2) При получении принт-сервером от Пользователя А и Пользователя В печатных заданий процесс печати приостанавливается.

3) Принт-сервер ожидает, пока некоторый пользователь авторизуется на «Сетевом контроллере» путем ввода пользователем своих аутентификационных данных.

4) Пользователь А подходит к «Сетевому контроллеру», который расположен в непосредственной близости с МФУ или принтером, это дает ему возможность визуально контролировать процесс печати. Пользователь вводит свои аутентификационные данные для авторизации в системе.

5) С устройства идентификационные данные через сеть попадают на принт-сервер, где проходят проверку на правомерность осуществляемых операций.

6) Принт-сервер проверяет в очереди печати наличие заданий для Пользователя А, который авторизовался на «Сетевом контроллере» (из принтерного задания можно получить информацию, в том числе, и о собственнике документа).

7) При наличии в очереди задания для Пользователя А (Printjob (А')) принт-сервер передает пакеты данных на «Сетевой контроллер», который в свою очередь передает пакеты данных непосредственно на устройство печати. Задание Пользователя В (Printjob (В')) остается в очереди на принт-сервере, до тех пор пока Пользователь В не авторизуется в системе.

8) Пользователь А забирает свой документ из лотка печатающего устройства.

В случае авторизации Пользователя В алгоритм процесса печати для него будет также одинаков и последователен, как и для пользователя А.

Рассмотренное решение обеспечения безопасности процессов печати может представлять интерес для средних и крупных организаций, где существует высокая степень рисков ИБ, связанных с утечкой конфиденциальных данных. Система помогает обеспечить необходимый уровень безопасности документооборота, минимизировать риски и эффективнее управлять печатью.

Литература

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы (4-е издание). — СПб, 2010.

Information security printing processes

A. S. Ryabov
OKB SAPR JSC, Moscow, Russia

The article is devoted to the problem of information security printing processes. The problems associated with leaking confidential information when you print the document on network printers. Offered technology secure printing, allowing to minimize risks of information security, by authorization of users in the print infrastructure.

Keywords: document management, information leakage, printing with authorization, printer, print server, network controller.

Bibliography —1 reference. *Received June 14, 2014*