

ОБЗОР ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ DLP-СИСТЕМЫ

Иванов О.П.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Научный руководитель – преподаватель Кривоносова Н.В.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Тезисы направлены на обзор неспецифичных возможностей DLP-системы, будут полезны системным администраторам компаний.

Одним из современных решений в организации защиты информации от внутренних угроз информационной безопасности являются DLP системы. На сегодняшний день есть много готовых «коробочных» решений, которые могут быть внедрены в компании для:

- избирательной блокировки локальных каналов передачи данных и каналов сетевых коммуникаций;
- мониторинга всех каналов утечки информации в сценариях работы пользователей;
- инспекции содержимого перемещаемых данных в режиме реального времени с возможностью блокировки такой попытки или отправки тревожного оповещения;
- обнаружения документов с критическим содержанием в различных местах хранения данных;
- выполнения заданных политик в равной степени как внутри корпоративного периметра;
- наличия аналитического инструментария для анализа предотвращенных попыток противоправных действий и случившихся инцидентов;
- защиты от преднамеренных или случайных действий пользователя, направленных на вмешательство в работу DLP-системы.

Основная цель предотвращения утечек конфиденциальной информации DLP – это выполнение всех требований политики конфиденциальности и безопасности информации, которые имеются в организации. Но кроме указанного функционала возможны и дополнительные возможности системы, то есть помимо основных задач DLP системы можно использовать для:

- анализа загруженности персонала: многие DLP-системы способны вести учет рабочего времени сотрудников, процесс каждого рабочего можно представить в виде статистики, которая показывает вовлечённость в процесс;
- обеспечения юридической поддержки: при наличии судебного разбирательства, DLP система предоставит доказательства злоумышленной деятельности;
- DLP как инструмент мотивации: когда сотрудники знают, что их действия находятся под контролем, появляется большая ответственность за рабочий процесс;
- DLP как хранилище.

Внедрение DLP-систем очень сложное и кропотливое занятие, которое требует достаточно много времени и ресурсов. Это не только возможность блокировать передачу конфиденциальной информации по различным каналам, но и возможность оптимальной организации работы сотрудников и резервного копирования информации.