СИСТЕМА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тарабаш Н.А.

Дворникова Т.Н. – м.т.н., старший преподаватель

Информация в наше время является наиболее ценным ресурсом и поэтому сегодня достаточно сложно встретить компании, которые не уделяют должного внимания вопросам защиты информации. Безопасность информации и предотвращение ее потери представляет серьезную проблему для компаний, поскольку число инцидентов, как и затраты на устранение их последствий, продолжает расти.

Конфиденциальная информация является критически важным объектом любой организации, а ее утечка может негативно сказаться на нематериальных активах компании и ее деловой репутации. Для предотвращения утечек данных внедряется автоматизированная корпоративная политика, которая захватывает защищенные данные до того, как она покинет границы корпоративной сети. Такое решение известно, как предотвращение потери данных или DLP (Data Loss Prevention).

Предотвращение потери данных идентифицирует, контролирует и защищает передачу данных путем глубокой проверки содержимого и анализа параметров транзакций (таких как источник, место назначения, объект данных и протокол) с централизованной структурой управления. В общем случае, обнаруживает и предотвращает несанкционированную передачу конфиденциальной информации.

Функциональные возможности DLP – системы

Одной из главных тенденций развития является переход от «заплаточных» систем, состоящих из компонентов от различных производителей, решающих каждый свою задачу, к единым интегрированным программным комплексам. Причина подобного перехода очевидна: комплексные интегрированные системы избавляют специалистов по информационной безопасности от необходимости решать проблемы совместимости различных компонентов «заплаточной» системы между собой, позволяют легко изменять настройки сразу для больших массивов клиентских рабочих станций в организациях, а также позволяют не испытывать сложностей при переносе данных из одного компонента единой интегрированной системы в другой. Также движение разработчиков к интегрированным системам идет в силу специфики задач обеспечения информационной безопасности: ведь если оставить без контроля хотя бы один канал, по которому может произойти утечка информации, нельзя говорить о защищенности организации от подобного рода угроз.

Еще одной важной тенденцией в сфере DLP является постепенный переход к модульной структуре, когда заказчик может самостоятельно выбрать те компоненты системы, которые ему необходимы (например, если на уровне операционной системы отключена поддержка внешних устройств, то нет необходимости доплачивать за функциональность по их контролю).