DLP – СИСТЕМЫ

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

Бородюк О.В., Михальков Н.В.

Бойправ О.В. – м.т.н.

В последнее время упоминания об утечках информации из самых разных организаций (коммерческих, некоммерческих, государственных и прочих) в новостных лентах информационных агентств и Интернет становятся фактически ежедневными. В связи с ростом таких инцидентов растет и интерес к системам, которые могли бы противостоять подобного рода угрозам.

Идеального решения по защите от внутренних угроз не существует — все зависит от требований, заложенных в политиках ИБ. Для реализации этих политик могут использоваться продукты пяти различных классов: системы блокировки портов, системы контроля доступа, криптосистемы, DLP-системы и IrM-системы. В мировой практике информационной безопасности считается, что наиболее действенными системами являются DLP-системы (Data Loss/Leak Prevention), так как они позволяют обеспечить не только защиту конфиденциальной информации в местах ее хранения, но и дают возможность контролировать данные в процессе их обработки и передачи.

DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности, или, иными словами, на защиту корпоративной информации от инсайдеров. Инсайдерами являются абсолютно все сотрудники компании, ведь утечки могут происходить не только по злому умыслу, но и по невнимательности сотрудников или незнанию правил информационной безопасности. Согласно статистике, свыше 80 % зарегистрированных инцидентов приходится именно на случайные утечки.

Основной признак любой современной DLP-системы — способность анализировать информацию, передаваемую по различным коммуникационным каналам, на предмет ее конфиденциальности. Фактически DLP-система — своеобразный черный ящик, на вход которого поступает информация, а в результате выдается вердикт — является ли она конфиденциальной. В дальнейшем на основе такого анализа система принимает решение: разрешить ли эту передачу данных или заблокировать ее.

Существует два основных подхода к анализу информации в DLP-системах. Первый – контентный подход предполагает, что из каждого передающегося файла извлекается текстовая составляющая, которая в дальнейшем каким-то образом исследуется. Второй — контейнерный метод, в его рамках анализируется не информация, а ее атрибуты, такие как тип файла, его размер, время создания или имя владельца. Другим примером контекстной фильтрации является использование специальных меток конфиденциальности, которые инкапсулируются в каждый защищаемый документ.

Необходимо также разделять комплексные DLP-системы и отдельные DLP-функции других систем безопасности. В частности, комплексная DLP-система должна поддерживать все основные исходящие коммуникационные каналы, иметь централизованную консоль управления и настройки политик, а также предоставлять возможность блокирования нежелательных перемещений информации. Это означает, что многие системы, использующие анализ контента, DLP-системами не являются, поскольку указанные функции представляют собой лишь одну из реализованных возможностей.

Одним из главных аспектов выбора и внедрения DLP-системы является ее совместимость с принципами и требованиями работы всей компании, ведь она имеет свои собственные стандарты безопасности, организацию работы IT-структуры, свои собственные, часто уникальные принципы ведения бизнеса. Всю информацию, имеющуюся в сети компании, можно подразделить на несколько типов:

– неклассифицированная;
– общедоступная информация;
– конфиденциальная, но не критичная;
– строго конфиденциальная информация.

Информация каждого из указанных типов требует определенных методов обработки и защиты.

Список использованных источников:

1. Tadviser [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.tadviser.ru/.
2. InfoWatch [Электронный ресурс]. – Электронные данные. – Режим доступа : www.infowatch.ru.
3. Softline [Электронный ресурс]. – Электронные данные. – Режим доступа : http://softline.ru/.
4. SolarSecurity [Электронный ресурс]. – Электронные данные. – Режим доступа : http://solarsecurity.ru/.