

Знаки конфиденциальности

Computerworld Россия, Валерий Коржов, 4.10.11

Ассоциация "DLP-Эксперт" обсуждает проект стандарта, который позволил бы пользователям помечать документы



В конце сентября ассоциация «DLP-Эксперт» провела круглый стол, посвященный обсуждению целесообразности разработки стандарта на метки конфиденциальности (элемент информации, характеризующий конфиденциальность информации, содержащейся в объекте), которые могли бы считывать и пользователи, и автоматизированные системы. Такие метки помогут добросовестным пользователям, допущенным к корпоративным секретам, случайно не нарушить режим обработки документов. Технология не предназначена для защиты от преднамеренных утечек, но дает пользователю возможность более ответственно работать с конфиденциальными документами.

Основных свойств такой метки два: ее должно быть сложно удалить случайно и она должна автоматически переноситься при копировании или другой модификации информации. Николай Федотов, ведущий аналитик компании **InfoWatch**, предлагает использовать набор технологий, позволяющий включать метки в сам текст, например предупреждение о его конфиденциальности, либо помещать в атрибутах файлов или в виде стеганографической информации, встроенной в основные данные. Не исключено, что проверка уровня конфиденциальности документа может быть реализована в виде веб-сервиса с использованием устойчивых к модификации текста хэш-функций. Существенным является то, что стандарт описания конфиденциальности открыт, и любой разработчик текстового редактора, операционной системы, файлового менеджера, автора мультимедийного кода может взять этот стандарт и реализовать в своем продукте. Кроме того, необходимо предусмотреть возможность отмечать подобными метками конфиденциальности как файл-контейнеры, так и потоки мультимедийной информации или базы данных. Метки такого рода, в отличие от используемых сегодня грифов секретности, могут быть не текстовыми последовательностями, но специальным набором символов, который легко проверить при автоматизированной обработке, но вероятность формирования которого случайным образом минимальна.

Подобные метки упрощали бы классификацию документов для систем DLP (Data Leak Protection — «защита от утечки данных») и применение правил работы с конфиденциальными документами различных уровней секретности.

Пока подобных стандартов на уровне рекомендаций RFC или документов МСЭ нет. Однако вполне возможно описать подобные метки в виде универсальных указателей на унифицированные идентификаторы ресурсов URI, микроформатов или пространств имен XML. Похожий стандарт уже разработан в рамках форума Forum of Incident Response and Security Teams для описания уровня опасности уязвимости — CVSS версии 2. Однако его можно переосмыслить и для указания опасности данных: утечка секретной информации вполне может быть поставлена в соответствие с уязвимостью по степени опасности и уровню риска. Однако, скорее всего, переосмысление это может быть разным, и на него можно разработать отдельный стандарт. Удобство CVSS еще и в том,



что он не только устанавливает уровни опасности, но и метрики для определения степени изменения риска в зависимости от времени и места расположения уязвимости (конфиденциальной информации).

Впрочем, многие члены «DLP-Эксперта» относятся к предложению **InfoWatch** со скепсисом. Они сомневаются, что метки на документах будут размещать сами пользователи, доверие к которым в вопросах информационной безопасности минимально. Многие считают, что пользователи будут игнорировать данный дополнительный инструмент и просто не обратят внимания ни на метки, ни на предупреждения защиты. Ну а для злоумышленников, которые проникнут в систему, будет хороший способ быстро найти наиболее ценную информацию — достаточно провести поиск по соответствующим меткам. Тем не менее эксперты выразили заинтересованность в разработке подобного стандарта, поскольку это еще один дополнительный инструмент, позволяющий предупредить пользователей об опасности бесконтрольного распространения информации.

Оригинал публикации: <http://www.osp.ru/news/articles/2011/10/13010626/>