Развитие DLP в России: история, тенденции и перспективы

Текст: **Сергей Петренко,** руководитель направления систем информационной безопасности ООО «ИТЕРАНЕТ»

В последние годы российский рынок DLP-систем переживает бурный рост. Вендоры активно расширяют функционал своих продуктов, начальники подразделений информационной безопасности разрабатывают корпоративные политики по предотвращению утечек конфиденциальных данных. Естественно, в такой ситуации не обходится без коллизий.


Сергей Петренко

На протяжении последних лет наблюдалась следующая интересная картина. Лет пять назад клиентам приходилось объяснять, что такое DLP-система (Data Leak Prevention, система предотвращения утечек данных) и почему она им жизненно необходима. Продукт, как правило, достаточно сильно кастомизировали под конкретного покупателя, и каждое внедрение было уникальным с технической точки зрения. Однако сегодня бизнес «распробовал» новую технологию: теперь уже клиенты активно инициируют внедрение DLP-систем, обращаются к разным вендорам, проводят тестирования продуктов, сравнивают характеристики и жаждут широчайшего набора разнообразных функций по контролю всего и вся.

Произошло это по следующим причинам. Во-первых, сам по себе посыл предотвращения утечек информации из корпоративной сети не совсем тривиален. Фактически впервые в истории защиты информации периметр сети защищают от пересечения изнутри, а не снаружи, то есть некий «умеренно доверенный» внутренний пользователь стал рассматриваться как активный источник угрозы утечки информации. Появилась задача контролировать невероятно широкий набор каналов передачи информации, которые ранее относительно свободно и бесконтрольно использовались сотрудниками в корпоративной информационно-телекоммуникационной системе. Во-вторых, DLP-системы опять же впервые предложили проводить анализ именно смыслового содержания информации – некий псевдоинтеллектуальный анализ. Соответственно, DLP-продукты изначально создавались с мощными «движками», располагающими широкими возможностями для разбора тех или иных информационных потоков до состояния текста, пригодного для смыслового анализа.

Постепенно к DLP-системам стали добавляться все новые и новые функции. Если начинали все с анализа почтовых сообщений и http-трафика, то в скором времени под влиянием требований пользователей нормой стали такие функции, как контроль всевозможных мессенджеров и USB-устройств, поиск информации в локальных и сетевых папках и т.д. В определенный момент времени клиенты уверовали во «всесильность» DLP-систем, и текущие ожидания потребителей стали обгонять возможности разработчиков по быстрому наращиванию функционала.

В настоящее время вендоры постоянно развивают функционал своих DLP-систем во всевозможных направлениях анализа информационных потоков и предотвращения утечек информации. Это развитие охватывает такие направления как:

- режимы работы (мониторинг, блокировка, автономный режим);
- режимы перехвата (на шлюзе, через агентов на ПК, «в разрыв» сети);
- возможности интеграции (Active Directory, почтовые и прокси-серверы, виртуальные среды);
- контролируемые каналы (корпоративная электронная почта, веб-почта, мессенджеры, социальные сети, протоколы туннелирования, внешние устройства, протоколы аутентификации);
- варианты реакции на инциденты (уведомление, блокирование, карантин);
- аналитические возможности (поиск по составным регулярным выражениям, поддержка опечаток, деобфускация).

И это далеко не полный список…

Ситуация осложняется тем, что относительно требований к DLP-системам нет единой теоретической базы, нет российского стандарта, который бы четко разграничивал, что входит в компетенции DLP, а что нет.

В итоге, развитие отечественных DLP-систем идет весьма хаотично и своеобразно. Некоторые вендоры идут «на поводу» у крупных корпоративных клиентов и включают в функционал своих систем те или иные возможности, имеющие весьма отдаленное отношение к утечкам данных. Например, контроль действий пользователей (снимки экрана, запись звука с микрофона ноутбука, кейлоггеры и т.д.). На наш взгляд, это, во-первых, имеет весьма косвенное

отношение к предотвращению утечек информации и, во-вторых, вызывает ряд вопросов нормативного и этического характера.

Другие разработчики (в их числе компания ИТЕРАНЕТ), прислушиваясь к пожеланиям и ожиданиям конечных пользователей, продолжают развивать профильный функционал DLP-систем. В частности, мы развиваем продукт в следующих направлениях:

- создание масштабируемой сетевой архитектуры (территориальной, программной, аппаратной), позволяющей развертывать DLP-системы на сложных распределенных корпоративных сетях и обеспечивать необходимый гибкий баланс централизации управления и автономности работы;
- отслеживание новых популярных средств обмена информацией и оперативное добавление функционала по их анализу;
- расширение перечня декодируемых протоколов (шифрованные протоколы, протоколы туннелирования и аутентификации);
- переход на отечественные (в том числе доверенные) СУБД и др.

История создания DLP-системы Business Guardian компанией ИТЕРАНЕТ – наглядный пример развития системы с позиции ожиданий потенциальных пользователей, потребностей общества, специфики социальных процессов, происходящих в нем. Например, первая версия BG была разработана в интересах промышленного холдинга, которому требовался только контроль SMTP–трафика. Для другого клиента – госзаказчика – была создана версия, которая включала уже в себя протокол HTTP/FTP и потребовала распределенной архитектуры. Выход на коммерческий рынок обеспечивала следующая версия BG, поддерживающая скорости выше 1 Гбит/с. А в настоящее время – это коммерческий коробочный продукт, включающий как функции DLP, так и решающий задачи поиска информации на каналах связи, в социальных сетях, форумах.

Пример «социального проекта» с использованием BG – работа по поиску утечек – производилась в период сдачи ЕГЭ по основным предметам в 2013 году. Площадка исследования – ВКонтакте (vk.com). Результат оценивался как поток сообщений в период проведения экзамена:

- предложений о продаже – до 400 в час;
- уникальных предложений – до 50 в час;
- наборов ответов – до 10 в час.

Таким образом, сейчас каждый российский разработчик DLP-систем развивается в соответствии с некой собственной уникальной программой, не привязанной к каким-либо единым стандартам или рекомендациям. При этом сами направления развития зачастую сильно различаются.

Ввиду отсутствия отраслевых стандартов на российском рынке пока не наблюдается ярко выраженных нишевых игроков. Но эта ситуация в скором времени должна измениться. Во-первых, готовятся к выходу рекомендации Банка России по предотвращению утечек, которые, как полагают эксперты, будут содержать соответствующие модель угроз и меры по защите. Во-вторых, ожидается выход руководящего документа ФСТЭК России «Требования к средствам защиты от несанкционированной передачи (вывода) информации», который, в свою очередь, определит классы защиты DLP-систем и требования к их функционалу. После принятия этих двух документов возможно профилирование ряда DLP-решений под соответствующие сферы применения (банковский сектор, государственные информационные системы, ИСПДн).

Кроме того, в отличие от западного рынка, у нас пока не просматривается тенденция к интеграции DLP-систем с другими средствами защиты информации: межсетевыми экранами, средствами обнаружения и предотвращения вторжений, антивирусными средствами и т.д. Возможно, это связано с отсутствием на российском рынке действительно крупных многопрофильных вендоров, которые могли бы позволить себе скупать более мелкие, но интересные технические решения. А может быть, дело в специфике российского бизнеса. Ведь большинство отечественных вендоров было основано и в настоящее время возглавляется вполне конкретными людьми, считающими выпускаемый продукт своим детищем и психологически не готовыми к продаже своего интеллектуального продукта или его частичному раскрытию для интеграции с чем-либо.

В целом же российский рынок DLP-систем, несмотря на бурный рост (как финансовый, так и технический), все еще находится на распутье, и направление его дальнейшего развития имеет множество вариантов. Многое зависит от регуляторов (свое слово, например, еще может сказать ФСБ России), немало зависит от позиции вендоров относительно пожеланий заказчиков по развитию непрофильного для предотвращения утечек функционала. DLP-системы могут как вырождаться в средства контроля за действиями пользователей, так и эволюционировать в высокоинтеллектуальные механизмы предотвращения внутренних угроз информационной безопасности.